

CAI
ZI
-2006
I050

V.4

Government
Publications

**Commission of Inquiry
into the Investigation of the
Bombing of Air India Flight 182**


**Research Papers
Volume 4**

**The Unique Challenges of Terrorism Prosecutions:
Towards a Workable Relation Between
Intelligence and Evidence**



3 1761 11651447 2





Digitized by the Internet Archive
in 2023 with funding from
University of Toronto

<https://archive.org/details/31761116514472>

Commission
of Inquiry into
the Investigation
of the Bombing of
Air India Flight 182



Commission d'enquête
relative aux mesures
d'investigation prises à
la suite de l'attentat à la
bombe commis contre
le vol 182 d'Air India

The opinions expressed in these academic studies are those of the authors;
they do not necessarily represent the views of the Commissioner.



©Her Majesty the Queen in Right of Canada, represented by the
Minister of Public Works and Government Services, 2010

Cat. No: CP32-89/5-2010E
ISBN: 978-0-660-19984-9

Available through your local bookseller or through
Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario
K1A 0S5

Telephone: (613) 941-5995 or 1 800 635-7943
Fax: (613) 954-5779 or 1 800 565-7757
publications@pwgsc.gc.ca
Internet: www.publications.gc.ca

Table of Contents

| | |
|---|------|
| Introduction | 1 |
| Chapter 1: The Fundamentals of Terrorism Prosecutions | 15 |
| 1.1 The Evolving Landscape: Terrorism, Security, Intelligence, and Evidence | 15 |
| 1.2 The Macdonald Case | 20 |
| 1.3 The 9/11 Case | 25 |
| 1.4 The 2001 Case | 30 |
| 1.5 The 2002 Case | 35 |
| 1.6 The 2003 Case | 40 |
| 1.7 The 2004 Case | 45 |
| 1.8 The 2005 Case | 50 |
| 1.9 The 2006 Case | 55 |
| 1.10 The 2007 Case | 60 |
| 1.11 The 2008 Case | 65 |
| 1.12 The 2009 Case | 70 |
| 1.13 The 2010 Case | 75 |
| 1.14 The 2011 Case | 80 |
| 1.15 The 2012 Case | 85 |
| 1.16 The 2013 Case | 90 |
| 1.17 The 2014 Case | 95 |
| 1.18 The 2015 Case | 100 |
| 1.19 The 2016 Case | 105 |
| 1.20 The 2017 Case | 110 |
| 1.21 The 2018 Case | 115 |
| 1.22 The 2019 Case | 120 |
| 1.23 The 2020 Case | 125 |
| 1.24 The 2021 Case | 130 |
| 1.25 The 2022 Case | 135 |
| 1.26 The 2023 Case | 140 |
| 1.27 The 2024 Case | 145 |
| 1.28 The 2025 Case | 150 |
| 1.29 The 2026 Case | 155 |
| 1.30 The 2027 Case | 160 |
| 1.31 The 2028 Case | 165 |
| 1.32 The 2029 Case | 170 |
| 1.33 The 2030 Case | 175 |
| 1.34 The 2031 Case | 180 |
| 1.35 The 2032 Case | 185 |
| 1.36 The 2033 Case | 190 |
| 1.37 The 2034 Case | 195 |
| 1.38 The 2035 Case | 200 |
| 1.39 The 2036 Case | 205 |
| 1.40 The 2037 Case | 210 |
| 1.41 The 2038 Case | 215 |
| 1.42 The 2039 Case | 220 |
| 1.43 The 2040 Case | 225 |
| 1.44 The 2041 Case | 230 |
| 1.45 The 2042 Case | 235 |
| 1.46 The 2043 Case | 240 |
| 1.47 The 2044 Case | 245 |
| 1.48 The 2045 Case | 250 |
| 1.49 The 2046 Case | 255 |
| 1.50 The 2047 Case | 260 |
| 1.51 The 2048 Case | 265 |
| 1.52 The 2049 Case | 270 |
| 1.53 The 2050 Case | 275 |
| 1.54 The 2051 Case | 280 |
| 1.55 The 2052 Case | 285 |
| 1.56 The 2053 Case | 290 |
| 1.57 The 2054 Case | 295 |
| 1.58 The 2055 Case | 300 |
| 1.59 The 2056 Case | 305 |
| 1.60 The 2057 Case | 310 |
| 1.61 The 2058 Case | 315 |
| 1.62 The 2059 Case | 320 |
| 1.63 The 2060 Case | 325 |
| 1.64 The 2061 Case | 330 |
| 1.65 The 2062 Case | 335 |
| 1.66 The 2063 Case | 340 |
| 1.67 The 2064 Case | 345 |
| 1.68 The 2065 Case | 350 |
| 1.69 The 2066 Case | 355 |
| 1.70 The 2067 Case | 360 |
| 1.71 The 2068 Case | 365 |
| 1.72 The 2069 Case | 370 |
| 1.73 The 2070 Case | 375 |
| 1.74 The 2071 Case | 380 |
| 1.75 The 2072 Case | 385 |
| 1.76 The 2073 Case | 390 |
| 1.77 The 2074 Case | 395 |
| 1.78 The 2075 Case | 400 |
| 1.79 The 2076 Case | 405 |
| 1.80 The 2077 Case | 410 |
| 1.81 The 2078 Case | 415 |
| 1.82 The 2079 Case | 420 |
| 1.83 The 2080 Case | 425 |
| 1.84 The 2081 Case | 430 |
| 1.85 The 2082 Case | 435 |
| 1.86 The 2083 Case | 440 |
| 1.87 The 2084 Case | 445 |
| 1.88 The 2085 Case | 450 |
| 1.89 The 2086 Case | 455 |
| 1.90 The 2087 Case | 460 |
| 1.91 The 2088 Case | 465 |
| 1.92 The 2089 Case | 470 |
| 1.93 The 2090 Case | 475 |
| 1.94 The 2091 Case | 480 |
| 1.95 The 2092 Case | 485 |
| 1.96 The 2093 Case | 490 |
| 1.97 The 2094 Case | 495 |
| 1.98 The 2095 Case | 500 |
| 1.99 The 2096 Case | 505 |
| 1.100 The 2097 Case | 510 |
| 1.101 The 2098 Case | 515 |
| 1.102 The 2099 Case | 520 |
| 1.103 The 2100 Case | 525 |
| 1.104 The 2101 Case | 530 |
| 1.105 The 2102 Case | 535 |
| 1.106 The 2103 Case | 540 |
| 1.107 The 2104 Case | 545 |
| 1.108 The 2105 Case | 550 |
| 1.109 The 2106 Case | 555 |
| 1.110 The 2107 Case | 560 |
| 1.111 The 2108 Case | 565 |
| 1.112 The 2109 Case | 570 |
| 1.113 The 2110 Case | 575 |
| 1.114 The 2111 Case | 580 |
| 1.115 The 2112 Case | 585 |
| 1.116 The 2113 Case | 590 |
| 1.117 The 2114 Case | 595 |
| 1.118 The 2115 Case | 600 |
| 1.119 The 2116 Case | 605 |
| 1.120 The 2117 Case | 610 |
| 1.121 The 2118 Case | 615 |
| 1.122 The 2119 Case | 620 |
| 1.123 The 2120 Case | 625 |
| 1.124 The 2121 Case | 630 |
| 1.125 The 2122 Case | 635 |
| 1.126 The 2123 Case | 640 |
| 1.127 The 2124 Case | 645 |
| 1.128 The 2125 Case | 650 |
| 1.129 The 2126 Case | 655 |
| 1.130 The 2127 Case | 660 |
| 1.131 The 2128 Case | 665 |
| 1.132 The 2129 Case | 670 |
| 1.133 The 2130 Case | 675 |
| 1.134 The 2131 Case | 680 |
| 1.135 The 2132 Case | 685 |
| 1.136 The 2133 Case | 690 |
| 1.137 The 2134 Case | 695 |
| 1.138 The 2135 Case | 700 |
| 1.139 The 2136 Case | 705 |
| 1.140 The 2137 Case | 710 |
| 1.141 The 2138 Case | 715 |
| 1.142 The 2139 Case | 720 |
| 1.143 The 2140 Case | 725 |
| 1.144 The 2141 Case | 730 |
| 1.145 The 2142 Case | 735 |
| 1.146 The 2143 Case | 740 |
| 1.147 The 2144 Case | 745 |
| 1.148 The 2145 Case | 750 |
| 1.149 The 2146 Case | 755 |
| 1.150 The 2147 Case | 760 |
| 1.151 The 2148 Case | 765 |
| 1.152 The 2149 Case | 770 |
| 1.153 The 2150 Case | 775 |
| 1.154 The 2151 Case | 780 |
| 1.155 The 2152 Case | 785 |
| 1.156 The 2153 Case | 790 |
| 1.157 The 2154 Case | 795 |
| 1.158 The 2155 Case | 800 |
| 1.159 The 2156 Case | 805 |
| 1.160 The 2157 Case | 810 |
| 1.161 The 2158 Case | 815 |
| 1.162 The 2159 Case | 820 |
| 1.163 The 2160 Case | 825 |
| 1.164 The 2161 Case | 830 |
| 1.165 The 2162 Case | 835 |
| 1.166 The 2163 Case | 840 |
| 1.167 The 2164 Case | 845 |
| 1.168 The 2165 Case | 850 |
| 1.169 The 2166 Case | 855 |
| 1.170 The 2167 Case | 860 |
| 1.171 The 2168 Case | 865 |
| 1.172 The 2169 Case | 870 |
| 1.173 The 2170 Case | 875 |
| 1.174 The 2171 Case | 880 |
| 1.175 The 2172 Case | 885 |
| 1.176 The 2173 Case | 890 |
| 1.177 The 2174 Case | 895 |
| 1.178 The 2175 Case | 900 |
| 1.179 The 2176 Case | 905 |
| 1.180 The 2177 Case | 910 |
| 1.181 The 2178 Case | 915 |
| 1.182 The 2179 Case | 920 |
| 1.183 The 2180 Case | 925 |
| 1.184 The 2181 Case | 930 |
| 1.185 The 2182 Case | 935 |
| 1.186 The 2183 Case | 940 |
| 1.187 The 2184 Case | 945 |
| 1.188 The 2185 Case | 950 |
| 1.189 The 2186 Case | 955 |
| 1.190 The 2187 Case | 960 |
| 1.191 The 2188 Case | 965 |
| 1.192 The 2189 Case | 970 |
| 1.193 The 2190 Case | 975 |
| 1.194 The 2191 Case | 980 |
| 1.195 The 2192 Case | 985 |
| 1.196 The 2193 Case | 990 |
| 1.197 The 2194 Case | 995 |
| 1.198 The 2195 Case | 1000 |
| 1.199 The 2196 Case | 1005 |
| 1.200 The 2197 Case | 1010 |
| 1.201 The 2198 Case | 1015 |
| 1.202 The 2199 Case | 1020 |
| 1.203 The 2200 Case | 1025 |
| 1.204 The 2201 Case | 1030 |
| 1.205 The 2202 Case | 1035 |
| 1.206 The 2203 Case | 1040 |
| 1.207 The 2204 Case | 1045 |
| 1.208 The 2205 Case | 1050 |
| 1.209 The 2206 Case | 1055 |
| 1.210 The 2207 Case | 1060 |
| 1.211 The 2208 Case | 1065 |
| 1.212 The 2209 Case | 1070 |
| 1.213 The 2210 Case | 1075 |
| 1.214 The 2211 Case | 1080 |
| 1.215 The 2212 Case | 1085 |
| 1.216 The 2213 Case | 1090 |
| 1.217 The 2214 Case | 1095 |
| 1.218 The 2215 Case | 1100 |
| 1.219 The 2216 Case | 1105 |
| 1.220 The 2217 Case | 1110 |
| 1.221 The 2218 Case | 1115 |
| 1.222 The 2219 Case | 1120 |
| 1.223 The 2220 Case | 1125 |
| 1.224 The 2221 Case | 1130 |
| 1.225 The 2222 Case | 1135 |
| 1.226 The 2223 Case | 1140 |
| 1.227 The 2224 Case | 1145 |
| 1.228 The 2225 Case | 1150 |
| 1.229 The 2226 Case | 1155 |
| 1.230 The 2227 Case | 1160 |
| 1.231 The 2228 Case | 1165 |
| 1.232 The 2229 Case | 1170 |
| 1.233 The 2230 Case | 1175 |
| 1.234 The 2231 Case | 1180 |
| 1.235 The 2232 Case | 1185 |
| 1.236 The 2233 Case | 1190 |
| 1.237 The 2234 Case | 1195 |
| 1.238 The 2235 Case | 1200 |
| 1.239 The 2236 Case | 1205 |
| 1.240 The 2237 Case | 1210 |
| 1.241 The 2238 Case | 1215 |
| 1.242 The 2239 Case | 1220 |
| 1.243 The 2240 Case | 1225 |
| 1.244 The 2241 Case | 1230 |
| 1.245 The 2242 Case | 1235 |
| 1.246 The 2243 Case | 1240 |
| 1.247 The 2244 Case | 1245 |
| 1.248 The 2245 Case | 1250 |
| 1.249 The 2246 Case | 1255 |
| 1.250 The 2247 Case | 1260 |
| 1.251 The 2248 Case | 1265 |
| 1.252 The 2249 Case | 1270 |
| 1.253 The 2250 Case | 1275 |
| 1.254 The 2251 Case | 1280 |
| 1.255 The 2252 Case | 1285 |
| 1.256 The 2253 Case | 1290 |
| 1.257 The 2254 Case | 1295 |
| 1.258 The 2255 Case | 1300 |
| 1.259 The 2256 Case | 1305 |
| 1.260 The 2257 Case | 1310 |
| 1.261 The 2258 Case | 1315 |
| 1.262 The 2259 Case | 1320 |
| 1.263 The 2260 Case | 1325 |
| 1.264 The 2261 Case | 1330 |
| 1.265 The 2262 Case | 1335 |
| 1.266 The 2263 Case | 1340 |
| 1.267 The 2264 Case | 1345 |
| 1.268 The 2265 Case | 1350 |
| 1.269 The 2266 Case | 1355 |
| 1.270 The 2267 Case | 1360 |
| 1.271 The 2268 Case | 1365 |
| 1.272 The 2269 Case | 1370 |
| 1.273 The 2270 Case | 1375 |
| 1.274 The 2271 Case | 1380 |
| 1.275 The 2272 Case | 1385 |
| 1.276 The 2273 Case | 1390 |
| 1.277 The 2274 Case | 1395 |
| 1.278 The 2275 Case | 1400 |
| 1.279 The 2276 Case | 1405 |
| 1.280 The 2277 Case | 1410 |
| 1.281 The 2278 Case | 1415 |
| 1.282 The 2279 Case | 1420 |
| 1.283 The 2280 Case | 1425 |
| 1.284 The 2281 Case | 1430 |
| 1.285 The 2282 Case | 1435 |
| 1.286 The 2283 Case | 1440 |
| 1.287 The 2284 Case | 1445 |
| 1.288 The 2285 Case | 1450 |
| 1.289 The 2286 Case | 1455 |
| 1.290 The 2287 Case | 1460 |
| 1.291 The 2288 Case | 1465 |
| 1.292 The 2289 Case | 1470 |
| 1.293 The 2290 Case | 1475 |
| 1.294 The 2291 Case | 1480 |
| 1.295 The 2292 Case | 1485 |
| 1.296 The 2293 Case | 1490 |
| 1.297 The 2294 Case | 1495 |
| 1.298 The 2295 Case | 1500 |
| 1.299 The 2296 Case | 1505 |
| 1.300 The 2297 Case | 1510 |
| 1.301 The 2298 Case | 1515 |
| 1.302 The 2299 Case | 1520 |
| 1.303 The 2300 Case | 1525 |
| 1.304 The 2301 Case | 1530 |
| 1.305 The 2302 Case | 1535 |
| 1.306 The 2303 Case | 1540 |
| 1.307 The 2304 Case | 1545 |
| 1.308 The 2305 Case | 1550 |
| 1.309 The 2306 Case | 1555 |
| 1.310 The 2307 Case | 1560 |
| 1.311 The 2308 Case | 1565 |
| 1.312 The 2309 Case | 1570 |
| 1.313 The 2310 Case | 1575 |
| 1.314 The 2311 Case | 1580 |
| 1.315 The 2312 Case | 1585 |
| 1.316 The 2313 Case | 1590 |
| 1.317 The 2314 Case | 1595 |
| 1.318 The 2315 Case | 1600 |
| 1.319 The 2316 Case | 1605 |
| 1.320 The 2317 Case | 1610 |
| 1.321 The 2318 Case | 1615 |
| 1.322 The 2319 Case | 1620 |
| 1.323 The 2320 Case | 1625 |
| 1.324 The 2321 Case | 1630 |
| 1.325 The 2322 Case | 1635 |
| 1.326 The 2323 Case | 1640 |
| 1.327 The 2324 Case | 1645 |
| 1.328 The 2325 Case | 1650 |
| 1.329 The 2326 Case | 1655 |
| 1.330 The 2327 Case | 1660 |
| 1.331 The 2328 Case | 1665 |
| 1.332 The 2329 Case | 1670 |
| 1.333 The 2330 Case | 1675 |
| 1.334 The 2331 Case | 1680 |
| 1.335 The 2332 Case | 1685 |
| 1.336 The 2333 Case | 1690 |
| 1.337 The 2334 Case | 1695 |
| 1.338 The 2335 Case | 1700 |
| 1.339 The 2336 Case | 1705 |
| 1.340 The 2337 Case | 1710 |
| 1.341 The 2338 Case | 1715 |
| 1.342 The 2339 Case | 1720 |
| 1.343 The 2340 Case | 1725 |
| 1.344 The 2341 Case | 1730 |
| 1.345 The 2342 Case | 1735 |
| 1.346 The 2343 Case | 1740 |
| 1.347 The 2344 Case | 1745 |
| 1.348 The 2345 Case | 1750 |
| 1.349 The 2346 Case | 1755 |
| 1.350 The 2347 Case | 1760 |
| 1.351 The 2348 Case | 1765 |
| 1.352 The 2349 Case | 1770 |
| 1.353 The 2350 Case | 1775 |
| 1.354 The 2351 Case | 1780 |
| 1.355 The 2352 Case | 1785 |
| 1.356 The 2353 Case | 1790 |
| 1.357 The 2354 Case | 1795 |
| 1.358 The 2355 Case | 1800 |

Table of Contents

| | |
|--|-----------|
| Introduction | 11 |
| Outline of the Paper | 17 |
| I. The Evolving Distinction Between Security Intelligence and Evidence | 22 |
| A) The Mackenzie Commission | 22 |
| B) The McDonald Commission | 23 |
| C) The Pitfield Committee | 24 |
| D) The 1984 CSIS Act and the Security Offences Act | 25 |
| E) The Distinction Between Evidence and Intelligence in the Post- Air India Bombing Period | 28 |
| F) Initial Recognition of the Problems of Converting Intelligence into Evidence | 33 |
| G) SIRC Reports on the Air India Investigation and RCMP/CSIS Co-Operation | 36 |
| H) Post 9/11 Understandings of the Distinction Between Evidence and Intelligence | 41 |
| 1. American Responses | 41 |
| 2. British Responses | 43 |
| 3. Canadian Responses | 47 |
| i) The Anti-Terrorism Act | 47 |
| ii) The Rae Report | 49 |
| iii) CSIS and the Conversion of Intelligence to Evidence | 51 |
| iv) The Arar Commission | 57 |
| v) The 2006 RCMP/CSIS MOU | 62 |
| I) Summary | 63 |
| II. Fundamental Principles Concerning Intelligence and Evidence | 64 |
| A) The Need to Keep Secrets | 65 |
| B) The Need to Treat the Accused Fairly | 69 |
| C) Respect for the Presumption of Open Courts | 78 |
| D) The Need for Efficient Court Processes | 83 |
| E) Summary | 87 |

| | |
|---|-----|
| III. The Use of Intelligence as Evidence | 87 |
| A) A Comparison Between <i>CSIS Act</i> and Criminal Code Electronic Surveillance Warrants | 88 |
| B) The Constitutionality of Warrants Issued Under Section 21 of the <i>CSIS Act</i> | 90 |
| 1. Section 8 of the Charter | 90 |
| 2. Section 1 of the Charter | 93 |
| 3. Section 24(2) of the Charter | 96 |
| 4. Use and Disclosure of a CSIS Warrant: A Case Study of <i>R. v. Atwal</i> | 97 |
| 5. Summary on the Admission of CSIS Wiretaps | 103 |
| C) The Case for Earlier Use of Criminal Code Electronic Surveillance Warrants | 103 |
| D) <i>R. v. Parmar</i> - A Case Study of Disclosure and Criminal Code Warrants | 105 |
| E) Disclosure and the Use of Special Advocates in Challenging CSIS and Criminal Code Warrants | 113 |
| F) The Collection and Retention of Intelligence under Section 12 of the <i>CSIS Act</i> | 116 |
| G) Admission of CSIS Information under Business Records Exceptions | 121 |
| H) Intelligence Collected Outside of Canada | 122 |
| 1. CSIS Wiretaps Directed at Activities Outside Canada | 122 |
| 2. Intelligence Collected by CSE Pursuant to Ministerial Authorization | 123 |
| 3. The Admissibility of Foreign Signals Intelligence | 126 |
| I. Summary | 127 |
| IV. Obligations to Disclose Intelligence | 129 |
| A) Disclosure of Intelligence under <i>R. v. Stinchcombe</i> | 130 |
| 1. The Scope of the Right to Disclosure | 132 |
| 2. The Relation Between the Rights of Disclosure and the Right to Full Answer and Defence | 137 |
| 3. <i>Stinchcombe</i> and the Duty to Preserve Evidence | 139 |
| 4. The Application of <i>Stinchcombe</i> Principles in the <i>Air India</i> Prosecution | 141 |
| 5. Subsequent Litigation Involving CSIS Destruction of Intelligence | 144 |
| B) Production and Disclosure of Intelligence as Third Party Records under <i>R. v. O'Connor</i> | 146 |
| C) Summary | 149 |

| | |
|---|-----|
| V. Methods of Restricting the Disclosure of Intelligence | 150 |
| A) Legislative Clarifications of <i>Stinchcombe</i> | 151 |
| B) Legislative Restrictions on Disclosure and Production under <i>Stinchcombe</i> and <i>O'Connor</i> | 152 |
| C) Disclosure and the Protection of Informers and Witnesses | 158 |
| D) <i>R. v. Khela</i> : A Case Study of the Limits of Police Informer Privilege and the Failure to Make Full Disclosure | 160 |
| E) Use of Privileges as a Means to Restrict Disclosure Obligations | 169 |
| 1. Expansion of Police Informer Privilege | 169 |
| 2. Creation of a New National Security Class Privilege for Intelligence | 171 |
| 3. Case- by- Case Privilege to Protect Intelligence | 172 |
| F) Summary | 173 |
| VI. Judicial Procedures to Obtain Non-Disclosure Orders | 175 |
| A) Section 37 of the CEA and Specified Public Interest Immunity | 176 |
| B) Section 38 of the CEA and National Security Confidentiality | 181 |
| 1. The Procedure under Section 38 of the Canada Evidence Act | 181 |
| 2. Notice Obligations and Disclosure Agreements | 181 |
| 3. Ex Parte Submissions and Special Advocates | 182 |
| 4. Reconciling the Interests in Secrecy and Disclosure under Section 38.06 | 188 |
| 5. Appeals under Section 38 | 189 |
| 6. Certificates Issued by the Attorney General to Prevent Court Ordered Disclosure | 190 |
| 7. Powers of Trial Judges to Protect Fair Trials under Section 38.14 | 190 |
| 8. Summary | 191 |
| C) Commentary on Section 38 of the Canada Evidence Act | 192 |
| D) Traditional Cold War Approaches to National Security Confidentiality | 195 |
| E) Evolving Approaches to National Security and the Dangers of Overclaiming Secrecy | 197 |
| 1. Changing Approaches to the Third Party Rule | 199 |
| 2. Changing Approaches to the Mosaic Effect | 202 |
| 3. Towards More Disciplined Harm-Based Approach to Disclosure | 204 |
| 4. Increasing Adversarial Challenge in the Section 38 Process | 207 |

| | |
|--|-----|
| 5. Increasing Transparency in the Section 38 Process | 209 |
| F) Non Disclosure of CSIS Material Not Seen by the Trial Judge: A Case study of <i>R. v. Kevork</i> | 210 |
| G) Use of Section 38 During a Criminal Trial: A Case Study of <i>R. v. Ribic</i> | 222 |
| 1. Federal Court Pre-Trial Proceedings Over Disclosure | 223 |
| 2. The Proceedings in Relation to the Witnesses that Ribic Proposed to Call at Trial | 227 |
| 3. The Federal Court of Appeal's Three Step Approach to National Security Confidentiality | 230 |
| 4. The Matter Returns to the Criminal Trial Judge | 234 |
| 5. Trial within a Reasonable Time Issues | 236 |
| 6. Summary | 239 |
| H) Use of Section 38 Before A Criminal Trial: A Case Study of <i>R. v. Khawaja</i> | 239 |
| 1. The Charter Challenge to Section 38 | 243 |
| 2. Two Rounds of Section 38 Hearings and an Appeal | |
| I) Summary | 251 |
| VII. Disclosure and Secrecy in other Jurisdictions | 254 |
| A) United States | 254 |
| 1. Disclosure Requirements | 254 |
| 2. Classified Information Procedures Act | 255 |
| 3. Security Clearances for Defence Lawyers | 256 |
| 4. Notice Provisions | 259 |
| 5. Means of Reconciling Secrecy with Disclosure | 259 |
| 6. Remedies for Non-Disclosure | 261 |
| 7. Interlocutory Appeals | 261 |
| 8. The Management of the Relation between Intelligence and Evidence and Tensions Between Intelligence Agencies and Prosecutors | 262 |
| 9. Summary | 264 |
| B) United Kingdom | 265 |
| 1. Disclosure Requirements | 266 |
| 2. Public Interest Immunity | 267 |
| C) Australia | 275 |
| 1. Public Interest Immunity Cases | 275 |
| 2. The Australian Law Reform Commission's Report | 279 |
| 3. The National Security Information Act | 284 |

| | |
|--|-----|
| 4. The <i>Lodhi</i> Case: The Australian Legislation Tested in a Completed Prosecution | 288 |
| 5. Summary | 292 |
| Conclusions | 293 |
| A) The Evolving Relation Between Intelligence and Evidence | 293 |
| B) The Case Studies: Canada's Difficult Experience with Terrorism Prosecutions | 295 |
| C) Front and Back-End Strategies for Achieving a Workable Relation Between Intelligence and Evidence | 296 |
| D) Front- End Strategies to Make Intelligence Useable in Terrorism Prosecutions | 297 |
| 1. Collection of Intelligence With Regard to Evidentiary and Disclosure Standards | 297 |
| 2. Seeking Amendments of Caveats under the Third-Party Rule | 301 |
| 3. Greater Use of Criminal Code Wiretap Warrants | 302 |
| 4. Greater Use of Source and Witness Protection Programs | 304 |
| E) Back -End Strategies To Reconcile The Demands of Disclosure and Secrecy | 305 |
| 1. Clarifying Disclosure and Production Obligations | 305 |
| 2. Clarifying and Expanding Evidentiary Privileges that Shield Information from Disclosure | 308 |
| 3. Use of Special Advocates to Represent the Interests of the Accused in Challenging Warrants | 309 |
| 4. Confidential Disclosure and Inspection of Relevant Intelligence | 311 |
| 5. A Disciplined Harm-Based Approach to Secrecy Claims | 313 |
| 6. An Efficient and Fair One Court Process for Determining National Security Confidentiality Claims | 315 |
| A One Court Approach: Superior Trial Court or Federal Court? | 318 |
| 7. Abolishing Pre-Trial Appeals | 321 |
| F) Conclusion | 322 |

The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation between Intelligence and Evidence

Kent Roach*

Introduction

The Commission of Inquiry Into the Investigation of the Bombing of Air India Flight 182 has been asked to examine “the manner in which the Canadian government should address the challenge, as revealed by the investigation and prosecutions in the Air India matter, of establishing a reliable and workable relationship between security intelligence and evidence that can be used in a criminal trial” and “whether the unique challenges presented by the prosecution of terrorism cases, as revealed by the prosecutions in the Air India matter, are adequately addressed by existing practices or legislation and, if not, the changes in practice or legislation that are required to address these challenges...”¹ This study, along with companion papers on structural and mega-trial aspects of terrorist trials,² and the American experience with terrorism prosecutions³, is designed to provide background for the Commission’s deliberations about how the many challenges presented by terrorism prosecutions may best be faced in the future.

The focus in this study will be on the unique challenges presented by terrorism prosecutions, as opposed to the common challenges presented by all complex and long criminal trials, especially those with multiple accused, multiple charges, multiple pre-trial motions and voluminous disclosure. Most of the unique problems of terrorism trials can be related to the difficulties of establishing a workable and reliable relationship between security intelligence and evidence that can be used in a criminal trial. The relation between intelligence and evidence inevitably implicates the relationship between security intelligence agencies and the police. Ultimately, there is an obligation to reconcile the need for secrecy with the need for disclosure. Legitimate needs for secrecy relate to intelligence sources, investigations, and restrictions or caveats placed

* Professor of Law, University of Toronto. Opinions expressed in this paper are those of the author and do not necessarily represent those of the Commission or Commissioner. I thank Birinder Singh and Robert Fairchild for providing excellent research assistance. A summary of this study is available in vol 3 of the Research Studies of the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.

1 Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 Terms of Reference May 1, 2006. b iii and vi.

2 Bruce MacFarlane Q.C. “Structural Aspects of Terrorist Trials” in Vol. 3 of the Research Studies

3 Robert Chesney “The American Experience with Terrorism Prosecutions” in Vol. 3 of the Research Studies.

on the use of intelligence by third parties. Legitimate needs for disclosure relate to the accused's rights to disclosure and full answer and defence and the public's right to a fair and public trial.

Security intelligence refers to information prepared by various agencies of the government, such as the Canadian Security Intelligence Service (CSIS) and foreign agencies, from closed and open sources about various risks to the national security of Canada. Security intelligence is generally secret and meant to alert officials to risks to national security in order to enable them to take effective preventive measures. Intelligence, for example, led to increased, but ultimately unsuccessful, precautions being taken in 1985 to protect Air India planes originating from Canada. Security intelligence is not collected with a view to its admissibility as evidence in court as proof of wrongdoing or its disclosure to the accused. Security intelligence may be based on hearsay reports of what some people have reported that they have heard others say. Security intelligence may also reveal highly sensitive and confidential methods and sources of covert intelligence gathering and other information that, if released, could harm Canada's national security or defence interests or its relations with other countries. Finally, security intelligence may be collected by methods that may not satisfy constitutional or common law standards that apply to the collection of evidence.

In contrast, evidence is collected by the police in the hope that it will result in the laying of charges and the transmission of evidence to prosecutors. Prosecutors have a duty to disclose relevant information to the accused, and to present evidence in open court in an attempt to prove beyond a reasonable doubt that the accused is guilty of a specific offence. Evidence is collected in accordance with various legal and constitutional standards, and the manner in which evidence is collected may become a subject of litigation as part of the trial process. Evidence is designed to be presented in court, where it will be subjected to adversarial challenge. Subject to certain limited exceptions such as the evidentiary privilege protecting police informers, the police assemble their files and evidence knowing that evidence will eventually be disclosed to the accused and presented in a public criminal trial.

Stated in the abstract, the differences between intelligence and evidence are stark. At the same time, the relation between intelligence and evidence is dynamic.⁴ Crimes related to terrorism often revolve around behaviour

⁴ Clive Walker "Intelligence and Anti-Terrorism Legislation in the United Kingdom" (2005) 44 *Crime, Law and Social Change* 387; Fred Manget "Intelligence and the Criminal Law System" (2006) 17 *Stanford Law and Public Policy Review* 415.

that may also be the legitimate object of the collection of security intelligence. Even before the enactment of the *Anti-Terrorism Act*, terrorism prosecutions could involve allegations of conspiracies or agreements to commit crimes or other forms of before-the-fact liability. The CSIS mandate has from the start included counter-terrorism investigations, and CSIS was created in the wake of high profile terrorist attacks -- including the October Crisis. The *Anti-Terrorism Act* now criminalizes support, preparation and facilitation of terrorism and participation in a terrorist group. The preventive nature of anti-terrorism law narrows the gap between intelligence about risks to national security and evidence about crimes.

The differences between security intelligence and admissible evidence present several challenges for terrorism prosecutions. A basic, and largely unexplored, question is whether security intelligence can be admitted as evidence in a criminal trial. This question involves the different standards that are used to obtain security intelligence and evidence under the Criminal Code.⁵ The Air India investigation raises questions about whether electronic surveillance obtained by CSIS could be admitted as evidence in a criminal trial. The possible admission of such intelligence as evidence also implicates issues of retention of intelligence and disclosure of intelligence to the accused.

Part of the value of security intelligence, especially intelligence based on vulnerable human sources, secret operations and information obtained from foreign agencies, is that it is kept confidential and is used by the government on a need-to-know basis. On the other hand, with respect to evidence to be used at a criminal trial and other relevant information, there are strong presumptions, backed up by the Canadian Charter of Rights and Freedoms, that it should be made public and disclosed to the accused in order to treat the accused fairly and to honour the open court principle. The constitutional disclosure obligations of the Crown to the accused go significantly beyond disclosing evidence to be used in the criminal trial to including other non-privileged information that is relevant to the case.⁶ The courts have also held that information used to obtain warrants should be disclosed to the accused in order to allow the accused to challenge the warrant.⁷ Even if security intelligence is not held, as it was in the *Malik and Bagri* trial, to be subject to disclosure

⁵ R.S.C. 1985 c.C-34 Part VI.

⁶ *R. v. Stinchcombe* [1991] 3 S.C.R. 326.

⁷ See *R. v. Parmar* (1987) 31 C.R.R. 256 and *R. v. Atwal* (1987) 36 C.C.C.(3d) 161 case studies discussed infra section 3.

obligations, the courts have recognized that the accused should have access to information held by third parties.⁸

Disclosure to the accused and the public is supported by the Charter, but it is not an absolute value. The Court has drawn a distinction between broad rights of disclosure under s.7 of the Charter and more limited principles that revolve around being able to know the case to meet and to make full answer and defence.⁹ Sections 37 and 38 of the *Canada Evidence Act* (CEA) provide procedures that allow the Attorney General of Canada (AG) to apply to courts to obtain orders for non-disclosure or modified disclosure of sensitive material. The Attorney General of Canada has a power under s.38.13 of the CEA to prevent even court-ordered disclosure of material received from foreign governments or disclosure of material that relates to national security or national defence. The discussion, in this paper, of the proper relation between security intelligence and evidence will require consideration of the accused's Charter rights to disclosure and full answer and defence, the open court principle protected under the Charter and the procedures that are available to maintain the confidentiality of security intelligence from disclosure to the accused and the public.

The importance and the difficulty of the many different issues raised by the relation between security intelligence and evidence cannot be underestimated. Taken together, they raise fundamental issues about the viability of criminal prosecutions for terrorism as well as about the important role of security intelligence that flows within and between governments. Both the law and the nature of intelligence should evolve to reflect the dangers of terrorism and the competing demands of secrecy and disclosure.

The relation between evidence and intelligence is dynamic. Our thinking about keeping secrets should evolve beyond a Cold War paradigm in which counter-intelligence dominated the work of security agencies and secrets about the enemy could be kept perhaps forever. The need to protect secrets takes on a new dimension when the targets of intelligence are about to blow airplanes out of the sky. Intelligence agencies must adapt to the new threat environment and the increased possibility that their counter-terrorism investigations may reach a point at which it is imperative to arrest and prosecute people. They must resist the

⁸ *R. v. O'Connor* [1995] 4 S.C.R. 401.

⁹ *R. v. Dixon* [1998] 1 S.C.R. 244; *R. v. Taillefer* [2003] 3 S.C.R. 307. On the importance of knowing the case to meet in the immigration context see *Charkaoui v. Canada* 2007 SCC 9.

temptation to engage in over-classification and unnecessary claims of secrecy. That said, the criminal process must also evolve to take account of the particular challenges of terrorism prosecutions. There is a need for efficient and fair means to require that only truly relevant information necessary for a fair trial must be disclosed to the accused. There must be an efficient and practical venue for the state to assert its interest in national security confidentiality. Both the intelligence and legal sides of the equation must change to respond to the challenges of international terrorism of which the 1985 Air India bombing was a horrific precursor.

Intelligence can be kept secret if it is only used to inform government of threats to national security.¹⁰ There is, however, a need to reconcile secrecy with fairness in cases where the intelligence becomes relevant in an accused's trial. At times, the Crown may want to introduce intelligence into evidence because it may constitute some of the best evidence of a terrorism crime. In many other cases, the accused may demand disclosure of intelligence on the basis that it will provide evidence that will assist the defence. A failure to disclose relevant evidence and information to the accused can threaten the fairness of the trial and can lead to wrongful convictions of innocent people. There have been wrongful convictions in the past in terrorism cases in other countries.¹¹ Canada must make every effort to avoid miscarriages of justice in the future. At the same time, the interests of justice are not served if the government is forced to disclose secret intelligence and information that is not necessary for the conduct of a fair trial. In such cases, the government will be placed in the unnecessary and impossible position of choosing between disclosing information that should be kept secret to protect sources, operations and foreign confidences or declining to bring terrorism prosecutions. This most difficult choice should only be necessary in cases where a fair trial is not possible without disclosure.

The choice between disclosure and prosecution is not a matter of hypothetical theory. In two prosecutions of alleged Sikh terrorists, the government essentially sacrificed criminal prosecutions rather than make full disclosure that would place informers at risk. One of these prosecutions involved Talwinder Singh Parmar, widely believed to have

¹⁰ The Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar has, however, stressed the need for review bodies to have access to secret material. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar *A New Review Mechanism for the National Security Activities of the RCMP* (Ottawa: Supply and Services, 2006).

¹¹ Bruce MacFarlane "Structural Aspects of Terrorist Trials" in Vol 3 of the Research Studies; Kent Roach and Gary Trotter "Miscarriages of Justice in the War Against Terrorism" (2005) 109 Penn. State Law Review 1001.

been the mastermind of the bombing of Flight 182. The other involved a conspiracy to blow up another Air India plane in 1986.¹² Although the Air India trial of Malik and Bagri did go to verdict in 2005, it could also have collapsed over issues of whether or not secrets had to be disclosed, had unprecedented steps not been taken to give the accused disclosure of secret material on conditional undertakings that the intelligence not be disclosed by the accuseds' lawyers to their clients.¹³ In addition, the trial judge did not have to order a remedy for the destruction of both wiretaps and notes by CSIS that should have been retained and disclosed to the accused only because he acquitted the accused.¹⁴ Other prosecutions in Canada, including the first prosecution under the 2001 *Anti-Terrorism Act* (ATA)¹⁵, have experienced difficulties and delay as a result of proceedings taken to obtain orders that intelligence or other secret information not be disclosed to the accused. Terrorism prosecutions may have to be abandoned unless the state is prepared to disclose information that is essential to a fair trial and unless there is a workable means to determine what information must be disclosed. Both intelligence agencies and the justice system need to adjust to the challenges of terrorism prosecutions.

Before the state is forced to abandon terrorism prosecutions in order to keep secrets, or a trial judge is forced to stay proceedings as a result of a partial or non-disclosure order, however, the justice system should ensure that the secret information is truly necessary for a just trial and that no other form of restricted disclosure will satisfy the demands of a fair trial. The public interest and the legitimate demands of the Charter will not be served by the unnecessary abandonment of criminal prosecutions in favour of preserving secrets which will not truly make a difference in the outcome or the fairness of the criminal trial. At the same time, the public interest and the legitimate demands of the Charter will not be served by unfair trials where information that should have been disclosed to, or introduced by, the accused is not available because of concerns about national security confidentiality, even if these concerns are legitimate.

The search for reasonable alternatives which can reconcile the demands of fairness and secrecy is not limited to the formal processes of the justice

¹² *R. v. Parmar* (1987) 31 C.R.R. 256 discussed *infra* section 3; *R. v. Khela* [1996] Q.J. no. 1940 discussed *infra* section 5.

¹³ Robert Wright and Michael Code "The Air India Trial: Lessons Learned". See also Michael Code "Problems of Process in Litigating Privilege Claims" in A. Bryant et al eds. *Law Society of Upper Canada Special Lectures The Law of Evidence* (Toronto: Irwin Law, 2004).

¹⁴ *R. v. Malik and Bagri* 2005 BCSC 350

¹⁵ *Canada. v. Khawaja* 2007 FC 463; *Canada. v. Khawaja* 2007 FC 490; *Canada. v. Khawaja* 2007 FCA 342; *Canada. v. Khawaja* 2007 FCA 388; *Canada v. Khawaja* 2008 FC 560 discussed *infra* section 6.

system. Efforts must be made to convince confidential informers that their identity can be revealed and that they will be protected through witness protection programs. Similarly, efforts must be made to persuade both domestic and foreign agencies to amend caveats that prohibit the use of their intelligence in court. The standard operating procedures of security intelligence agencies with respect to counter-terrorism investigations, including the use of warrants, the treatment of confidential sources and the recording of surveillance and interviews, should be reviewed in light of the disclosure and evidentiary demands of terrorism prosecutions. This does not mean that CSIS should become a police force.¹⁶ It does mean that CSIS should be aware of the evidential and disclosure demands of terrorism prosecutions. Reconciling the contradictory demands of fairness and secrecy is one of the most difficult and delicate tasks faced by prosecutors, security agencies, judges and society alike. It is also one of the most important tasks to accomplish if the criminal justice system is to be effectively deployed against terrorists.

Outline of the Paper

The first part of this paper will provide an historical outline of thinking about the distinction between security intelligence and evidence. Although stark contrasts between secret intelligence and public evidence have frequently been drawn, the 1984 *CSIS Act* did not contemplate a wall between intelligence and evidence. The Air India bombing and 9/11 have underlined the need for intelligence to be passed on to the police and, if necessary, for it to be used as evidence. At the same time, intelligence agencies have legitimate concerns that this could result in the disclosure of secrets in open court and to the accused. The respective roles of police and security intelligence agencies are grounded in principle and statute. At the same time, however, they are not set in stone and they continue to evolve. The distinction between proactive intelligence and reactive law enforcement that was conventional wisdom in 1984 may no longer be acceptable today. Any contemporary discussion of the distinction between security intelligence and evidence should account for the enactment of the *Anti-Terrorism Act* in 2001. This act was designed to give the police more tools to prevent terrorism before it happens: primarily through prosecutions of various crimes for financing, support, and preparation for terrorism.

¹⁶ For warnings about CSIS becoming a “stalking horse” or “proxy for law enforcement” see Stanley Cohen *Privacy, Crime and Terror Legal Rights and Security in a Time of Peril* (Toronto: LexisNexis, 2005) at 407.

The second part of this paper will outline some of the competing goals that should inform the relationship between security intelligence and evidence. These include: 1) the need to respect the confidential and highly sensitive nature of intelligence including methods, sources, ongoing investigations and information received from third parties; 2) the need to treat the accused fairly under the Charter especially with respect to the right to full answer and defence; 3) the need to respect the presumption that courts will be open to the public and the press; and 4) the need to ensure that criminal courts can efficiently and accurately reach verdicts in terrorism trials. Ultimately, there is a need to reconcile the need for secrecy with the need for disclosure.

Both secrecy and disclosure are very important. The disclosure of information that should be kept secret can result in harm to confidential informants, damage to Canada's relations with allies, and damage to information gathering and sharing that could be used to prevent lethal acts of terrorism. The non-disclosure of information can result in unfair trials and even wrongful convictions. Even if the disclosure of secret information is found to be essential to a fair trial, the Attorney General of Canada can prevent disclosure by issuing a certificate under s.38.13 of the *Canada Evidence Act* that blocks a court order of disclosure. The trial judge in turn can stay or stop the prosecution under s.38.14 if a fair trial is not possible because of non-disclosure.

Although most of the concern expressed about the relation between intelligence and evidence has been about keeping intelligence secret and protecting it from disclosure, there may be times when the state may want to use intelligence as evidence in terrorism trials. This raises the issue of whether information collected by CSIS, including information from CSIS wiretaps, as well as intercepts collected under ministerial authorization by the Communications Security Establishment (CSE), can be introduced into evidence. Intelligence is generally collected under less demanding standards than evidence and this presents challenges when the state seeks to use intelligence as evidence. In addition, the use of intelligence as evidence may require increased disclosure of how the intelligence was gathered. There are, however, provisions that allow public interests in non-disclosure to be protected but these may affect the admissibility of evidence. These issues, including maintaining the appropriate balance between CSIS and Criminal Code warrants, will be examined in the third part of this paper.

In order to focus discussion, relevant case studies will be used throughout this paper. In this third part, the case studies will include the abandoned prosecution against Talwinder Singh Parmar, and others, in relation to an alleged Hamilton plot to commit acts of terrorism in India, after the accused successfully sought access to an affidavit used to obtain a Criminal Code authorization to engage in electronic surveillance. The second case study examined in this part will be the Atwal case, involving attempted murder convictions and abandoned conspiracy to commit murder charges in relation to the shooting of Indian Cabinet minister Malkiat Singh Sindhu. *Atwal* remains the leading case with respect to the admissibility of CSIS wiretaps as evidence in criminal trials.

The fourth part of this paper will examine disclosure requirements as they may be applied to intelligence. In *R. v. Malik and Bagri*, CSIS material was held to be subject to disclosure by the Crown under *Stinchcombe*. *Stinchcombe* creates a broad constitutional duty for the state to retain and disclose relevant and non-privileged information to the accused. Even if, in other cases, CSIS is held not to be directly subject to *Stinchcombe* disclosure requirements, intelligence could be ordered disclosed and produced under the procedure that applies under *O'Connor* to records held by third parties. A significant amount of intelligence could be the subject of production and disclosure in a terrorism prosecution.

The fifth part of this paper will examine possible legislative restrictions on disclosure through the enactment of new legislation to limit *Stinchcombe* and *O'Connor*, and through the expansion or creation of evidentiary privileges that shield information from disclosure. The precedents for such restrictions on disclosure will be examined and attention will be paid to their consistency with the Charter rights of the accused, including the important role of innocence at stake exceptions to even the most important privileges. Attention will also be paid to the effects of restrictions on disclosure on the efficiency of the trial process. Disclosure restrictions may generate litigation over the precise scope of the restriction or privilege, as well as Charter challenges. Throughout this analysis, I will draw on the relevant experience, as revealed by the Air India prosecution, as well as other terrorism prosecutions, such as the *R. v. Khela* case, in which a stay of proceedings was eventually entered after the Crown failed for many years to reveal the identity of, and statements taken from, a key informant who participated in the discussions leading to the conspiracy charges with respect to an alleged plan to bomb another Air India plane in 1986.

The sixth part of this paper will examine existing means to secure non-disclosure orders to protect the secrecy of intelligence in particular prosecutions. This will involve the procedures contemplated for claiming public interest immunity and national security confidentiality under ss.37 and 38 of the *Canada Evidence Act*, as amended by the 2001 ATA. Section 38, like other comparable legislation, is designed to allow for the efficient and flexible resolution of competing interests in disclosure and non-disclosure. It provides for a flexible array of alternatives to full disclosure: agreements between the Attorney General and the accused, selective redactions, the use of summaries, and various remedial orders, including admissions and findings of facts, as well as stays of proceedings with respect to parts or all of the prosecution. A singular feature of s.38, however, is that it requires the litigation of national security confidentiality claims not in the criminal trial and appeal courts, but in the Federal Court. As will be seen, Canada's two-court approach differs from that taken in other countries. It requires a trial judge to be bound by a Federal court judge's ruling with respect to disclosure, while also reserving the right of the trial judge to order appropriate remedies, including stays of proceedings, to protect the accused's right to a fair trial. Although the s.38 procedure was not used in the *Air India* trial, it could have been used had prosecuting and defence counsel not been able to fashion an alternative regime of disclosure, subject to an initial undertaking that defence lawyers not disclose the evidence to their clients. The limited use of s.38 in terrorism prosecutions will be examined in the *Kevork* and *Khawaja* cases, as will its use in the *R. v. Ribic* prosecution relating to a hostage taking in Bosnia.

The seventh part of this paper will examine the procedures used in the United States, the United Kingdom and Australia to resolve claims of national security confidentiality, with a view to understanding how the approaches used in those countries differ from those used in Canada and whether they provide a sounder basis for maintaining a workable and reliable relationship between security intelligence and evidence. A striking feature of these comparative regimes is that they all allow a criminal trial court to resolve and revisit claims of national security confidentiality and consequent non or partial disclosure orders in light of the evolving nature of the criminal prosecution. In contrast, the Canadian approach contemplates the Federal Court making final and binding orders with respect to non-disclosure and the criminal trial court then deciding whether a fair trial is still possible in light of the Federal Court's non-disclosure orders.

The conclusion of this paper will assess strategies for making the relationship between intelligence and evidence workable. Both front-end strategies that address the practice of intelligence agencies and the police and back-end strategies that address disclosure obligations and the role of the courts are needed.

Some of the front-end strategies that could make intelligence more useable in terrorism prosecutions include: 1) culture change within security intelligence agencies that would make them pay greater attention to evidential standards when collecting information in counter-terrorism investigations; 2) seeking permission from originating agencies under the third party rule for the disclosure of intelligence; 3) greater use of Criminal Code wiretaps, as opposed to CSIS wiretaps in Canada, and the use of judicially authorized CSIS intercepts, as opposed to CSE intercepts, when terrorist suspects are subject to electronic surveillance outside of Canada; and 4) greater use of effective source and witness protection programs by intelligence agencies.

Some of the back-end strategies that could help protect intelligence from disclosure are: 1) clarifying disclosure and production standards in relation to intelligence; 2) clarifying evidential privileges; 3) providing a means by which secret material used to support a CSIS or a Criminal Code warrant can be used to support the warrant while subject to adversarial challenge by a security cleared special advocate; 4) providing for efficient means to allow defence counsel, perhaps with a security clearance and/or undertakings not to disclose, to inspect secret material; 5) focusing on the concrete harms of disclosure of secret information as opposed to dangers to the vague concepts of national security, national defence and international relations; 6) providing for a one-court process to determine claims of national security confidentiality that allows a trial judge to re-assess whether disclosure is required throughout the trial; and 7) abolishing the ability to appeal decisions about national security confidentiality before a terrorism trial has started.

All of these issues are united by the need to establish a reliable, workable and fair relationship between intelligence and evidence. They raise fundamental questions about the viability of criminal prosecutions as a response to the threats of, and to acts of, international terrorism such as that which resulted in the bombing of Air India Flight 182.

I. The Evolving Distinction Between Security Intelligence and Evidence

In this section, I will examine public thinking about the perceived difference between security intelligence and evidence and its relation to the distinct roles played by security intelligence agencies and police forces. I will take an historical approach in order to trace the evolution of thinking about the differences between security intelligence and evidence as we moved from a Cold World era that emphasized counter-intelligence against a hostile state, to a post 9/11 world, where the emphasis is on counter-terrorism against hostile non-state actors. The 1985 Air India bombing has a particular significance in this evolution. It was a tragic and horrific foreshadowing of the post 9/11 era. At the same time, it is not clear that our thinking about the relation between intelligence and evidence has evolved sufficiently to reflect the threat of terrorism or the need to prosecute terrorists.

A) The Mackenzie Commission

The first Canadian recommendation that the collection of security intelligence be separated from policing was made in 1969 by a Royal Commission on Security, commonly called the MacKenzie Commission after its chair. This Commission examined a number of different topics such as security clearances, immigration and security and external affairs and industrial security; none of which were focused on law enforcement. The Commission explained that the security procedures that it would examine:

...are not necessarily related to the detection and prosecution of illegalities, where precise legal definitions would be of central importance, but are mainly concerned with the collection of information and intelligence, with the prevention and detection of leakages of information and with prevention against attempts at subversion.¹⁷

It proposed the creation of a civilian intelligence agency with a preventive mandate that would be distinct from the more reactive law enforcement mandate of the police.

¹⁷ *Report of the Royal Commission on Security (Abridged)* (Ottawa: Information Canada, 1969) at para 4.

The Mackenzie Commission proposed that wiretapping for security reasons be exempted from proposed legislation enforcing the provision of judicial warrants, and that it be subject to Ministerial authorization. It concluded that “ministers are more readily aware of the full details of the cases brought to their attention, are in a better position to understand the special requirements of security, and could maintain more centralized control of the complete range of wiretapping operations.”¹⁸ It recognized that the new security intelligence agency “should, when necessary, operate in close liaison and co-operation with the RCMP and other police forces”¹⁹, but it did not deal with the difficulties of managing the relation between intelligence and evidence.

B) The McDonald Commission

The McDonald Commission examined RCMP activities, including unlawful activities, that were committed in the wake of the 1970 October Crisis, in which two terrorist cells in Quebec committed a kidnapping and a murder. It observed that some illegal acts were committed by the RCMP because “a feeling developed that, because the law could be applied only after offences were committed, the enforcement of the law was an inadequate means of effectively forestalling politically motivated acts of violence.”²⁰

The Commission recommended the creation of a civilian security intelligence agency that could investigate various threats to the security of Canada, including terrorism. The Commission defined security intelligence as “advance warning and advice about activities which threaten the internal security of Canada.”²¹ With respect to terrorism, the Commission observed:

Acts of political terrorism, when there is reason to believe they are about to occur or after they occur, are properly the concern of law enforcement agencies. But governments and police forces in Canada should have advance intelligence. Immigration authorities, for example, should have information about international

¹⁸ Ibid at para 292.

¹⁹ Ibid at para 297

²⁰ Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police *Freedom and Security under the Law* (Ottawa: Ministry of Supply and Services, 1981) at 269.

²¹ Ibid at 414.

terrorists to be able to identify them when they apply for entry to Canada...Canada, as a signatory to several international conventions concerning international co-operation in combating terrorism...is obliged to contribute to the international pool of intelligence about terrorists²²

The Commission stressed that security intelligence was the product both of information collected, often through covert investigations, and of “an analysis of the information based on an assessment of its significance in both a national and international context.”²³ It concluded that the security intelligence function should be located outside of the RCMP because of the need for political judgment and direction of security intelligence work and because of the dangers of combining police powers with the collection of security intelligence.²⁴ The McDonald Commission was more aware of terrorism than the Mackenzie Commission, which it noted had not even mentioned the word terrorism,²⁵ and it contemplated that the RCMP would play a continuing role in the investigation of offences relating to national security, including apprehended and actual acts of terrorism. Nevertheless, the McDonald Commission’s focus was not on the relationship that would emerge between a new civilian security agency and the police²⁶ or the relation between intelligence and evidence.

C) The Pitfield Committee

In 1983, a Special Senate Committee known as the Pitfield Committee after its chair, Senator Michael Pitfield, examined the distinction between intelligence and evidence at some length and in terms that continue to be influential. The Pitfield Committee stressed the differences between law enforcement and security intelligence:

Law enforcement is essentially reactive. While there is an element of information-gathering and prevention in law enforcement, on the whole it takes place after the commission of a distinct criminal offence. The protection of security relies less on reaction to events; it seeks advance warning of security threats, and is

²² *ibid* at 416

²³ *ibid* at 419

²⁴ *ibid* at 423, 614

²⁵ *ibid* at 40

²⁶ The McDonald Commission’s examination of the police focused on matters such as complaints, legal advice, police powers and the police’s relation with the Solicitor General. *Ibid* at 957-1053.

not necessarily concerned with breaches of the law. Considerable publicity accompanies and is an essential part of the enforcement of the law. Security intelligence work requires secrecy. Law enforcement is 'result-oriented', emphasizing apprehension and adjudication, and the players in the system- police, prosecutors, defence counsel, and the judiciary- operate with a high degree of autonomy. Security intelligence is, in contrast, 'information-oriented'. Participants have a much less clearly defined role, and direction and control within a hierarchical structure are vital. Finally, law enforcement is a virtually 'closed' system with finite limits- commission, detection, apprehension, adjudication. Security intelligence operations are much more open-ended. The emphasis is on investigation, analysis, and the formulation of intelligence.²⁷

The observations of the Pitfield Committee represent influential but flawed thinking about the distinction between law enforcement and intelligence at the time of the creation of CSIS, and this flawed thinking was also evident during the initial Air India investigation. Law enforcement was defined in narrowly reactive terms. Police and prosecutors were autonomous actors that entered the scene after a crime has been committed. The police independently collected evidence to be introduced in a public trial while security intelligence agencies subject to political direction proactively collected advance information about threats. The distinctions between intelligence and evidence collection could not have been stated more starkly. The proactive role of the police in preventing crime and in prosecuting attempts and conspiracies to commit acts of terrorism was ignored. Not surprisingly, the possibility that intelligence could have evidential value in a criminal trial was also ignored.

D) The 1984 CSIS Act and the Security Offences Act

CSIS was created in 1984 with a mandate to investigate a broad range of threats to the security of Canada. Although these threats to the security of Canada included threats and acts of serious violence directed at persons

²⁷ *Report of the Special Committee of the Senate on the Canadian Security Intelligence, Delicate Balance: A Security Intelligence Service in a Democratic Society* (Ottawa: Supply and Services Canada, 1983) at p.6 para 14.

or property for political ends within Canada or a foreign state, they also included espionage, clandestine foreign-influenced activities and the undermining by covert unlawful acts of the constitutionally established government of Canada. The *CSIS Act* was created during the Cold War, a context symbolized by reports that CSIS surveillance on Parmar was interrupted for surveillance of a visiting Soviet diplomat.²⁸

CSIS was created in a manner that allowed political direction and review and oversight of the new agency in a manner different from the norms that governed the relations between the police and the government.²⁹ CSIS can be tasked by the Minister of Defence and Minister of Foreign Affairs to provide information and intelligence in certain circumstances.³⁰ Section 12 of the *CSIS Act* contemplated that CSIS would collect information and intelligence about threats to the security of Canada under standards that differed from those used by the police. It provides that “the Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada.” The act specifically refers to information and intelligence as distinct from evidence and it predicates investigations on reasonable grounds of suspicion of threats to the security of Canada.

The *CSIS Act* provided for a separate warrant regime that specifically excluded the existing scheme under Part VI of the Criminal Code³¹. A CSIS wiretap warrant required reasonable grounds to conclude that electronic surveillance was required to investigate a threat to the security of Canada or to investigate foreign states or persons in matters in relation to the defence of Canada and the conduct of its international affairs, as opposed to reasonable grounds to believe that a crime had been committed and that the surveillance would reveal evidence of the crime.³² All of these matters distinguished the role of CSIS in providing security intelligence to the government from the role of the police in collecting evidence to justify the laying and prosecution of charges.

28 Kim Bolan *Loss of Faith How the Air India Bombers Got Away with Murder* (Toronto: McClelland and Stewart, 2005) at 63.

29 On the evolving norms of police independence which stress the legitimate role of transparent Ministerial directives to the police see Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar *A New Review Mechanism for the RCMP's National Security Activities* (2006) ch 9; *Report of the Upperwash Inquiry Policy Analysis* (2007) ch.12.

30 *CSIS Act* ss.13-16

31 *ibid* s.26

32 *ibid* s.21

The *CSIS Act* placed an emphasis on secrecy. It made it an offence to disclose information relating to a person “who is or was a confidential source of information or assistance to the Service” or Service employees “engaged in covert operational activities of the Service”³³. At the same time, the *CSIS Act* did not contemplate absolute secrecy or that intelligence would never be passed on to law enforcement. Section 19(2) of the *CSIS Act* provided that CSIS may disclose information to relevant police and prosecutors “where the information may be used in the investigation or prosecution of an alleged contravention of any law of Canada or a province...”³⁴ Even in 1984, there was a recognition that CSIS could have intelligence that would be useful in both criminal investigations and prosecutions. The *CSIS Act* did not establish an impermeable wall between intelligence and relevant information to be provided to the police. Its implicit understanding of the relation between the collection of intelligence and evidence was more complex and nuanced than the stark contrast articulated by the Pitfield committee.

The proactive role of the police in preventing and investigating crime in the national security area was also recognized in much less noticed companion legislation to the *CSIS Act*, the *Security Offences Act*³⁵. In that act, RCMP officers were given “the primary responsibility to perform the duties that are assigned to peace officers” in relation to offences that arise “out of conduct constituting a threat to the security of Canada” as defined in the *CSIS Act*. The duties of RCMP officers include the prevention of crime and the apprehension of offenders³⁶. A broad range of offences, including murder, attempted murder, other forms of violence or threatening, espionage, sabotage and treason could be involved in conduct that constitutes a threat to the security of Canada. In addition, the Criminal Code prohibits not only completed offences, but attempts beyond mere preparation to commit such offences, agreements or conspiracies between two or more people to commit offences and attempts to counsel, procure or instigate others to commit offences, as well as a broad range of assistance to criminal activity.

A close reading of the *CSIS Act* and the *Security Offences Act* suggests that the stark dichotomy that the Pitfield Committee made between reactive law enforcement and preventive intelligence gathering was simplistic. The foundational 1984 legislation contemplated the disclosure of intelligence to the police for use in criminal investigations

³³ Ibid s.18.

³⁴ Ibid s.19(2)(a).

³⁵ R.S.C. 1985 c.S-7 s.6.

³⁶ RCMP Act s.18

and prosecutions. It established overlapping jurisdictions by giving CSIS a mandate to investigate acts of terrorism, defined as threats and acts of serious violence directed at persons or property for political ends, that could both before and after completion constitute crimes. The RCMP was given primary jurisdiction over these crimes. Their role was not solely reactive because they had a mandate to prevent crime and they could investigate and lay charges both before and after acts of terrorism.

E) The Distinction Between Evidence and Intelligence in the Post Air India Bombing Period

A July 1984 MOU provided a bare-bones framework for the sharing of information between the RCMP and CSIS. After outlining areas where information could be shared, it provided that “neither CSIS nor the RCMP shall have an unrestricted right of access to the operational records of the other agency” and “shall not initiate action based on the information provided without the concurrence of the other agency.” The vague reference to “action” would presumably cover legal proceedings, but it could also cover a broad range of investigative activities. The MOU went on to provide that “operational information” from joint operations of the RCMP and CSIS “shall be freely shared between the two agencies” but with “source and third party information excepted.”³⁷

A more comprehensive 1986 MOU devoted a chapter to information sharing between the two agencies. It contemplated that a Deputy Director of CSIS and a Deputy Commissioner in the RCMP would “interface” with respect to information sharing, but that “Any disagreement regarding the sharing of information or the action to be taken based on such information not resolved by the Director (CSIS) and the Commissioner (RCMP) shall be referred to the Solicitor General (or his designate) for resolution.” The fact that both the RCMP and CSIS were under the direction of the same Minister provided the potential for resolving disputes over information sharing and the subsequent use of information. The Solicitor General, in consultation with Cabinet, could ultimately decide whether it was more important to keep secrets or bring prosecutions.

Unlike the 1984 MOU, the 1986 MOU specifically tracked s.19(2) of the *CSIS Act* by providing that CSIS agreed to provide “information to the RCMP:

³⁷ MOU signed July 17, 1984 pub doc RCMP 00001.0352

- i. relevant to the investigation and enforcement of alleged security offences or the apprehension thereof which fall under the primary responsibility of the RCMP pursuant to s.6(1) of the *Security Offences Act*³⁸

This provision recognized that both the *CSIS Act* and the *Security Offences Act* contemplated a continued national security role for the RCMP. At the same time, the MOU did not specifically address the treatment of the information provided by CSIS to the RCMP with respect to judicial proceedings. There was no reference to steps that could be taken to protect secret intelligence under the *Canada Evidence Act*.

In 1987, a Special Senate Committee on Terrorism and Public Safety commented on reports alleging a lack of co-operation “between federal police and intelligence-gathering agencies on one hand and (provincial) Crown prosecutors on the other in the prosecution of alleged terrorists.” It stated that there was “at least one instance where provincial Crown prosecutors failed to obtain a judgment against alleged terrorists at least in part due to CSIS’ decision not to allow its officers to testify or to disclose certain information.”³⁹ As will be seen in the subsequent parts of this study, a number of terrorism prosecutions had by this time collapsed or been strained over issues of disclosure of CSIS information or disclosure of informants.

The Special Senate Committee concluded that problems in the relation between CSIS and law enforcement bodies were related to a lack of understanding of CSIS’s role, which it described as being “essentially intelligence and information gathering for risk assessment” and not as being to “gather evidence to support criminal prosecutions.”⁴⁰ The Committee concluded that CSIS “should cooperate fully with provincial Crown prosecutors in the prosecution of alleged terrorists, but not to the extent of prejudicing the safety of CSIS officers, their contacts or of important, ongoing investigations.”⁴¹ This recommendation was not likely to solve problems or conflicts in the relation between CSIS and law enforcement, given the primacy that CSIS, as well as the *CSIS Act* itself, gave to the protection of the secrecy of its informants, its operations and its officers.

³⁸ MOU signed November 1986 Chapter 13.

³⁹ Chair Hon. William Kelly *Terrorism The Report of the Senate Special Committee on Terrorism and Public Safety* (Ottawa: Ministry of Supply and Services, 1987) at 41

⁴⁰ *ibid* at 41

⁴¹ *ibid* at 41

A recommendation that did have some potential for resolving conflicts between security intelligence agencies and the police was that the federal Attorney General assert jurisdiction in terrorism prosecutions that might involve CSIS information and witnesses. This recommendation could keep disputes about whether the public interest was best served by secrecy or disclosure within the federal government. Such disputes would involve the Solicitor General, with responsibility for both CSIS and the RCMP, and the Attorney General of Canada, with an independent responsibility to determine whether prosecutions were in the public interest. The assertion of federal preeminence with respect to terrorism prosecutions was contemplated in the *Security Offences Act*. Although it would not solve all the conflicts between disclosure and secrecy, it would keep them all under the same roof.

The 1987 Senate report essentially accepted the stark dichotomy between evidence and intelligence gathering that was reflected in the 1983 Pitfield report. It did not engage in a rethinking of the relation between intelligence and evidence in light of the Air India bombing. Although urging co-operation between the RCMP and CSIS, it maintained the primacy of protecting the confidentiality of CSIS investigations, agents and informers over the need to reveal such information and intelligence when required to do so in a criminal prosecution.

In 1987, the Independent Advisory Team on CSIS also confirmed a sharp distinction between the intelligence gathering and analysis functions of CSIS and the evidence gathering and prosecution functions of the police. In the course of recommending increased efforts towards civilianization and analysis, the Advisory Team summarized the “fundamental differences between security intelligence work and police work” as follows:

- police deal with facts (evidence) usually after the event, whereas security intelligence agencies try to anticipate events;
- police forces must have a degree of independence from Government control, whereas security intelligence agencies require closer control to ensure that individual rights are not unnecessarily infringed, and where they are infringed, to ensure that political accountability exists;

- police activities are subject to an extensive and detailed set of rules (the Criminal Code and jurisprudence), while security intelligence activities, though provided for by the *CSIS Act*, involve greater judgment in their implementation; and finally,
- a security intelligence agency must keep its Government informed of threats to national security, while police work will normally culminate in evidence being laid before a Crown Attorney for presentation to the Court.⁴²

The emphasis in this report was on improving CSIS's ability to collect and assess intelligence, and not on its ability to work with the police. Unfortunately, neither this report nor the Senate report of the same year addressed questions that were essential to the ongoing Air India investigation.

In its 1988-89 annual report, SIRC commented on some tensions between various police forces and CSIS. It explained:

With a mandate to bring criminals to justice, the police have reason to treat all information as potential evidence for production in court. CSIS has a different mandate, to gather information as a basis for advice to government, and is understandably anxious to protect information that could 'burn' a source.⁴³

These comments reaffirmed the traditional divide between the police mandate to collect evidence and the security intelligence mandate to collect confidential intelligence. This conventional wisdom was first articulated by the Pitfield Committee in 1983 and it did not appear to change after the 1985 Air India bombing.

In 1988 Addy J. addressed some of the differences between intelligence collected by CSIS and evidence collected for criminal investigations. In upholding the denial of disclosure of CSIS information in the course of a judicial review of a denial of a security clearance, he stated that:

⁴² *People and Process in Transition Report to the Solicitor General by the Independent Advisory Team on CSIS* October 1987 at 5.

⁴³ SIRC Annual Report 1989-1990 at 38.

the fundamental purpose of and indeed the *raison d'être* of a national security intelligence investigation is quite different and distinct from one pertaining to criminal law enforcement, where there generally exists a completed offence providing a framework within the perimeters of which investigations must take place and can readily be confined. Their purpose is the obtaining of legally admissible evidence for criminal prosecutions. Security investigations on the other hand are carried out in order to gather information and intelligence and are generally directed towards predicting future events by identifying patterns in both past and present events.

There are few limits upon the kinds of security information, often obtained on a long-term basis, which may prove useful in identifying a threat...An item of information, which by itself might appear to be rather innocuous, will often, when considered with other information, prove extremely useful and even vital in identifying a threat. The very nature and source of the information more often than not renders it completely inadmissible as evidence in any court of law. Some of the information comes from exchanges of information between friendly countries of the western world and the source of method by which it is obtained is seldom revealed by the informing country.

Criminal investigations are generally carried out on a comparatively short-term basis while security investigations are carried out on systemically over a period of years, as long as there is a reasonable suspicion of the existence of activities which could constitute a threat to the security of the nation....

[a]n informed reader may at times, by fitting a piece of apparently innocuous information from the general picture which he has before him, be in a position to arrive at some damaging deductions regarding the investigations of a particular threat or of many other threats to national security....⁴⁴

⁴⁴ *Henrie v. Canada (Security Intelligence Review Committee)* (1988) 53 D.L.R.(4th) 568 at 577-578 affd (1992) 88 D.L.R.(4th) 575 (Fed.C.A.)

Justice Addy argued that secret nature of intelligence, often received “from exchanges of information between friendly countries of the western world”, rendered it “completely inadmissible as evidence in any court of law.” His comments discounted the possibility that intelligence might have evidential value. As will be seen in a subsequent section, an attempt had already been made by this time to introduce CSIS wiretaps in a terrorism prosecution.⁴⁵ Justice Addy also demonstrated a concern about the mosaic effect of disclosing intelligence. The assumption was that “an informed reader”, probably intelligence agents of the Soviet Union or its allies, could piece together ongoing operations or sources from “apparently innocuous information.” As will be seen, Justice Addy also cited the mosaic effect in a 1984 case involving a terrorism prosecution⁴⁶ and ordered that CSIS material not be disclosed to the accused without even examining the material.

A refusal to consider the evidential value of security intelligence may have made some sense during the height of the Cold War. CSIS and its counterparts were primarily concerned with spying by the Soviet Union and its partners. Criminal prosecutions did not play an important role in this work. It did not, however, fit the nature of counter-terrorism work that could result in prosecutions of non-state actors. As the 1980’s drew to a close and the Soviet Union and its empire started to collapse, the conventional wisdom about the stark and absolute divide between secret intelligence and public evidence slowly began to be questioned.

F) Initial Recognition of the Problems of Converting Intelligence into Evidence

In 1990, a Special Committee of the House of Commons conducted a five-year review of the *CSIS Act*. This report recognized “the difficulties of serious technical problems to be overcome regarding the process by which intelligence generated by CSIS can be transformed into criminal evidence, especially in cases where politically motivated violence is concerned.”⁴⁷ The Committee reported complaints from the RCMP that while CSIS passed information to the RCMP, “the information received was often ‘too massaged’ to be of much real use.” The Committee raised concerns, however, about whether raw intelligence would put CSIS sources in jeopardy and “whether evidence obtained directly from CSIS sources and methods can be used successfully in court without a

⁴⁵ *R. v. Atwal* (1987) 36 C.C.C.(3d) 161 (Fed.C.A.).

⁴⁶ *Re Kevork* (1984) 17 C.C.C.(3d) 426 (F.C.T.D.) discussed *infra* Part IV

⁴⁷ *In Flux But Not in Crisis* at 105

Charter challenge.”⁴⁸ This raised concerns about different standards for authorizing electronic surveillance under the *CSIS Act* and the Criminal Code that will be discussed more fully in part 3 of this study, as well as concerns about the disclosure of CSIS informants and/ or officers that might be required in criminal prosecutions. Having identified some of the difficulties of converting intelligence into evidence that could be admitted and disclosed in terrorism prosecutions, however, the five year review Commons committee did not propose any solutions for addressing them.

A new MOU signed between the RCMP and the CSIS in 1990 also demonstrated increased awareness of the difficulties of managing the relation between secret intelligence and public evidence. Section 7 of this MOU provided:

The CSIS and the RCMP recognize that from time to time information and intelligence provided by the CSIS to the RCMP will have potential value as evidence in the investigation or prosecution of a criminal offence. Both parties further recognize that, given that CSIS does not normally collect information for evidentiary purposes, such use is exceptional and will not be considered without the prior approval of CSIS. When such use is taken, full account will be taken of the balance of public interest in the particular case, including the seriousness of the crime, the importance and uniqueness of the information provided by the CSIS, and the potential effects of disclosure on CSIS sources of information, methods of operations and third party relations.

This provision recognizes that, in “exceptional cases”, intelligence could be used as evidence and helpfully provided some public interest criteria to guide such decisions. The criteria speak both to the need and importance of the evidence in the particular case as well as the harm that the use of the evidence may cause to CSIS operations and third party relations.

Section 9 of the 1990 MOU also provided that pursuant to s.19(2)(a) of the *CSIS Act*, which contemplates CSIS provision of information to be used by the police in their investigations or prosecutions, that “CSIS agrees to provide ‘spin-off’ information and intelligence to the RCMP” relevant to

⁴⁸ *ibid* at 104

the investigation of indictable offences where the RCMP had jurisdiction over the offence. The meaning of ‘spin-off’ information and intelligence is not clear, but it seems to contemplate that primary information and intelligence collected by CSIS may not necessarily be disclosed. The MOU recognized that intelligence would be used in criminal prosecution, but only in “exceptional cases” and only as a “spin-off” from CSIS’s mandate to collect secret intelligence to inform the government about threats to national security.

Finally, section 24 of the MOU provided that in addition to respect for caveats and the confidentiality of information that:

Subject only to the requirements of the Courts, information provided by either party to this Memorandum of Understanding shall not be used for the purpose of obtaining search warrants or authorizations to intercept private communications, produced as evidence in Court proceedings or disclosed to Crown Prosecutors or any third-party without the prior express approval of the party that provided the information.

Nothing in this Memorandum of Understanding shall be interpreted as compelling either party to disclose the identity of its sources or caveated information from a third party.⁴⁹

This provision required CSIS or the RCMP to consent to information being used to obtain judicial warrants. This recognized that information used to obtain a judicial warrant would be subject to disclosure requirements in order to allow the accused to challenge the legality of the warrant. By that time, both the police and CSIS had experience with the disclosure of the information used to obtain both Criminal Code and CSIS wiretaps in terrorism investigations.⁵⁰

The 1990 MOU also required CSIS consent before such information was disclosed to prosecutors or used in court. As will be discussed in the fourth part of this study, however, the Supreme Court constitutionalized a broad right to disclosure in *Stinchcombe* in 1991; a year after the MOU was signed. Although information held by Crown prosecutors was

⁴⁹ MOU signed August 21, 1989 pub doc RCMP 0001.0352

⁵⁰ See the discussion of *R. v. Parmar* and *Atwal v. Canada* in Part 3 of this study.

subject to disclosure obligations, *Stinchcombe* in effect required full disclosure of relevant and non-privileged information held by the police about a case, whereas the MOU contemplated CSIS having a veto over whether information it disclosed to the police would in turn be disclosed to the prosecutor for possible disclosure to the accused. The 1990 MOU was catching up to the difficulties of managing the relation between intelligence and evidence, but its emphasis on secrecy and CSIS consent for the disclosure of information were still in tension with evolving disclosure requirements.

G) SIRC Reports on the Air India Investigation and RCMP/CSIS Co-Operation

The SIRC report on the bombing of Air India also considered matters related to the distinction between security intelligence and evidence. SIRC reported that CSIS officials had notified the RCMP about what they believed to be a one shot discharge of a rifle that was heard during the surveillance of Parmar and Reyat at Duncan. This was consistent with s.19(2) of the *CSIS Act* which contemplated that CSIS could transmit information that might be relevant to a criminal investigation to the police. In the aftermath of the bombing, SIRC expressed some concern that the senior management of CSIS did not clarify CSIS's mandate in relation to the RCMP or "set out CSIS policy on the sharing of information and intelligence with the RCMP."⁵¹ Despite the lack of policies regarding the sharing of information with the RCMP, SIRC related the post-bombing difficulties between the two agencies to differences of mandate. It stated:

As the investigation progressed, RCMP officials felt it necessary to examine certain CSIS files on certain Sikh extremist targets in more detail. *CSIS, whose mandate is to collect intelligence and not evidence, was at first reluctant to expose its files, and by extension its methods and sources, for any evidentiary use by the RCMP.* Lengthy negotiations took place between the two agencies, but eventually the RCMP investigators were allowed access to the files subject to some mutually agreed upon conditions on the subsequent use of the information.

⁵¹ Security Intelligence Review Committee Annual Report 1991-1992 (1992) at 10.

Overall, we found no evidence that access to CSIS information relevant to the RCMP investigation of the disaster was unreasonably denied to the Force.⁵²

SIRC also relied on its understanding of the CSIS mandate when evaluating CSIS's erasure of tapes of Parmar's electronic surveillance. Although criticizing the lack of clarity about CSIS's retention policy, it commented that an instruction "which removed from Service facilities the capacity to collect and preserve criminal evidence tapes" was "consistent with the provisions of the *CSIS Act* establishing the Service as an intelligence agency with no police powers or responsibilities."⁵³ Although the problems of converting intelligence into evidence had been identified by the five-year Parliamentary review committee, and in the 1990 MOU between the RCMP and CSIS, efforts to overcome these difficulties were countered by assumptions which relied on the different mandates of the RCMP and CSIS, and by the notion that intelligence would only be used in prosecutions in exceptional cases.

In 1998 and 1999, SIRC conducted a study of RCMP/CSIS relations. It noted that previous "difficulties and disagreements appear to centre mainly, but not entirely, on the exchange of information and intelligence between the RCMP and CSIS on operational matters and thus, if widespread or systemic, could affect cooperation at its most fundamental level."⁵⁴ This report outlined a system in which RCMP liaison officers at CSIS had access to much information, but to which caveats restricting the subsequent use of the information were generally attached. Even advisory letters from CSIS that contemplated the use of information to obtain a search warrant reserved the right of CSIS to challenge by any means the release of CSIS information without consultation and approval from CSIS.⁵⁵ SIRC commented:

At the root of the problems in the exchange of information between CSIS and the RCMP is the need for CSIS to protect information, the disclosure of which could reveal the identity of CSIS sources, expose its methods of operation or that could compromise ongoing CSIS investigations. On the other hand, some RCMP

52 *ibid* at 10 (*italics added*)

53 *ibid* at 11

54 CSIS Co-operation with the RCMP Part 1 (SIRC Study 1998-04) 16 October, 1998 at p.2.

55 *ibid* at 8.

investigators see some CSIS information as evidence that is vital to a successful prosecution, but which can be denied to them by caveats placed on the information by CSIS or that, even if used, will be subject to the Service invoking sections 37 and 38 of the Canada Evidence Act, an action that could seriously impede the RCMP's case. The Service view is that it does not collect evidence. This possible misunderstanding on the part of some RCMP investigators may result in certain CSIS information/intelligence being treated as though it were evidence but which might not stand up to Court scrutiny because it had not been collected to evidentiary standards.⁵⁶

In this passage, SIRC expressed concerns that CSIS information might not be admitted into criminal trials because it was not collected to evidentiary standards and that the use of ss.37 and 38 of the Canada Evidence Act to protect CSIS information from disclosure could threaten criminal prosecutions. As will be seen, these are serious and legitimate concerns. Nevertheless, they are concerns mainly for the prosecution. They should only affect CSIS to the extent that CSIS might be asked to alter its practices in some cases in order to collect information, such as physical surveillance, to evidentiary standards or to support the RCMP in obtaining Criminal Code search warrants. The root of the problem, as SIRC correctly noted, was not so much the difficulties in using intelligence in criminal prosecutions, though these might be considerable, but rather CSIS's unwillingness to expose its investigations, sources and officers to disclosure. The reluctance of CSIS to risk such disclosure had support in its mandate to collect secret intelligence and, in the offences in s.18 of the *CSIS Act*, to disclose confidential sources and covert operations. Nevertheless, any global defence of secrecy begged the question of whether in a particular case, prosecution and disclosure was in the public interest.

SIRC also noted that the concerns of both the RCMP and CSIS had been increased by the impact of the Supreme Court's 1991 decision in *Stinchcombe*. SIRC appended the full text of the decision to its report and commented that:

The impact of that decision is that all CSIS intelligence disclosures, regardless of whether they would be entered

⁵⁶ *ibid* at 9.

for evidentiary purposes by the Crown, are subject to disclosure to the Courts. Any passage of information, whether an oral disclosure or in a formal advisory letter, could expose CSIS investigations. This means that even information that is provided during joint discussions on investigations or that is provided as an investigative lead is at risk.⁵⁷

This was a very expansive and somewhat alarmist reading of the implications of *Stinchcombe*. Although *Stinchcombe* defined disclosure obligations broadly, it did not define them in an unlimited manner. Disclosure obligations were subject to qualifications based on relevance to the case, privilege, including informer privilege, as well as with respect to the timing of disclosure. In addition, the Attorney General of Canada could assert public interest immunity to prevent disclosure. Indeed, this had already been successfully done in at least one terrorism prosecution.⁵⁸

SIRC raised concerns about the decentralized nature of the RCMP that led to different interpretations of *Stinchcombe* disclosure obligations.⁵⁹ It may have been helpful in such circumstances to have gotten some consensus about the precise extent of disclosure obligations rather than to have assumed that they were very broad. SIRC's argument that *Stinchcombe* had made relations between CSIS and the RCMP worse also downplayed difficulties that had arisen in the relationship long before the Supreme Court's 1991 decision. A case in point that will be subsequently examined is the 1987 decision in *Atwal* that had led to the disclosure of information used to obtain a CSIS electronic surveillance warrant and the eventual resignation of the director of CSIS because of inaccuracies in that affidavit. Long before *Stinchcombe*, CSIS was aware that disclosure was a likely consequence of its involvement in terrorism prosecutions. Indeed, CSIS's initial experience with disclosure in the criminal justice system was a memorable, albeit unhappy one.

The SIRC report noted that CSIS was helping its employees prepare to testify in the Air India case. It raised concerns, however, that review of CSIS documents by the RCMP Air India task force "could potentially place an extensive amount of CSIS information at risk under the *Stinchcombe* ruling regardless of whether it was subsequently used as evidence."⁶⁰

⁵⁷ Ibid at 9.

⁵⁸ See the case study of the *Kevork* prosecution discussed infra Part VI.

⁵⁹ Ibid at 18.

⁶⁰ Ibid at 14-15.

This report turned out to be prescient as CSIS was found to be subject to *Stinchcombe* disclosure requirements at the Malik and Bagri trial.

A second study of regional co-operation completed in 1999 also revealed that RCMP officers were concerned that CSIS officers were not disclosing to them all that they should see. These concerns were, however, denied by CSIS officers.⁶¹ It also reported RCMP frustration that CSIS advisory letters authorized less disclosure than their initial disclosure letters. At the same time, SIRC concluded that CSIS's withholding of information to protect third party information, human sources and methods of operation "is consistent with Service policy, and is clearly stated in the terms of the Memorandum of Understanding."⁶² SIRC was told that O Division had reduced its requests for disclosure letters from CSIS by 90% in large part "because the *Stinchcombe* decision had effectively turned CSIS information into what was described as a 'poison pill' when a related prosecution was initiated" ⁶³ because of an unwillingness to disclose intelligence. It noted that some RCMP officers complained that CSIS was overprotective of its human sources, and that the police had experience with human sources and related issues of witness protection. SIRC described the disclosure issue as "what seems now to be an insoluble problem...that carried the potential to disrupt CSIS-RCMP relationships and could potentially damage the operation of both agencies."⁶⁴ The SIRC report seemed to contemplate legislation that would resolve the difficulties created by disclosure obligations, but did not outline how legislation could accomplish this task.

The 1998 and 1999 SIRC reports affirmed that the traditional divide between intelligence and evidence was still present and that concerns about compromising intelligence had been significantly expanded as a result of *Stinchcombe*. Although SIRC may have overestimated some of the impact of *Stinchcombe*, it was clear that many within the RCMP and CSIS believed that *Stinchcombe* had aggravated the tensions arising from the different mandates of the two agencies.

61 CSIS Cooperation with the RCMP- Part 2 (SIRC Study 1998-04) 12 Feb, 1999 at p. 5.

62 *ibid* at 6.

63 *ibid* at 7.

64 *ibid* at 18.

H) Post 9/11 Understandings of the Distinction Between Evidence and Intelligence

1. American Responses

The tension between the need to preserve the confidentiality of intelligence and the need to disclose evidence for trials is a universal feature of developed justice systems. As will be examined in greater detail in the seventh part of this study, many of Canada's allies have taken significant steps to facilitate the use of intelligence in criminal prosecutions. As early as 1986, one knowledgeable American commentator wrote:

Cases dealing with classified information often cause friction between the Justice Department and the intelligence agency which has information at stake. The conflict arises because intelligence agencies are uniformly reluctant to disclose classified information, even though this information might be necessary to successfully prosecute a case. The Justice Department, on the other hand, is reluctant to proceed without advance assurances that the intelligence agency involved will declassify the necessary information. These contrary positions frequently result in an impasse and the alleged wrongdoer going free.⁶⁵

In 1986 the conflicts between the desire to preserve the confidentiality of intelligence and to provide evidence were evident in cases in the United States, mainly in espionage cases and so-called greymail cases involving prosecutions of former officials who had access to classified information. One of the central and recurring questions for this study is whether there has been an adequate change in attitudes and practices towards intelligence and evidence in order to respond effectively and fairly to the challenges of terrorism prosecutions.

Although the United States does not have a separate domestic civilian intelligence agency such as CSIS, administrative barriers, colourfully, but not accurately, known as "the wall", were constructed to regulate the sharing of intelligence obtained under the *Foreign Intelligence Surveillance Act (FISA)* with prosecutors working on criminal prosecutions. Many of

⁶⁵ Brian Tamanaha "A Critical Review of The Classified Information Procedures Act" 1986, 13 Am. J. Crim. L. 277 at 280-281.

these barriers were created in the wake of concerns that the Aldrich Ames espionage case might have been threatened by law enforcement uses of FISA warrants. These restrictions were then interpreted to place barriers on sharing information between FBI agents working on FISA investigations and those working on regular criminal investigations. The barriers played some role in at least one investigation of one of the 9/11 hijackers. One FBI agent working on the intelligence side rebuffed an inquiry from another FBI agent working on the law enforcement side, in part because the file contained signals intelligence. The rebuffed FBI agent working on the law enforcement side replied that “someday someone will die- and wall or not- the public will not understand why we were not more effective... Lets hope the National Security Law Unit will stand behind their decisions then, since the biggest threat to us now, bin Laden, is getting the most ‘protection.’”⁶⁶

The 9/11 Commission found that the FBI intelligence agent who denied access about signals intelligence to another agent had confused matters because the suspect was already subject to a law enforcement investigation. Nevertheless, the 9/11 Commission still reached the chilling conclusion that more information sharing could have identified at least two of the hijackers and possibly disrupted the 9/11 plot.⁶⁷ It stated:

The perception evolved into the still more exaggerated belief that the FBI could not share *any* intelligence information with criminal investigators, even if no FISA procedures had been used. Thus, relevant information from the National Security Agency and the CIA often failed to make its way to criminal investigators. Separate reviews in 1999, 2000 and 2001 concluded independently that information sharing was not occurring... Finally the NSA began putting caveats on its Bin Ladin-related reports that required prior approval before sharing their contents with criminal investigators and prosecutors. These developments further blocked the arteries of information sharing.⁶⁸

A Joint Inquiry by Senate and House committees on intelligence also found problems with information sharing between intelligence agencies

⁶⁶ 9/11 Commission Report at 8.2.

⁶⁷ 9/11 Commission Report at 3.2.

⁶⁸ 9/11 Commission Report at 3.2.

and the FBI. It related this “breakdown of communications” to “differences in the agencies’ missions, legal authorities and cultures.”⁶⁹ Both the Joint Inquiry and an Inspector General’s report found that the CIA failed to pass on to the FBI information about the travel to the United States of two of the 9/11 hijackers. The Inspector General commented that such information and proper operational follow-through “might have resulted in surveillance of both al Mihdhar and Al-Hazmi, surveillance in turn, would have the potential to yield information on flight training, financing and links to others who were complicit in the 9/11 attacks.”⁷⁰

The 9/11 terrorist attacks underlined the importance of sharing intelligence with law enforcement. At the same time, the post 9/11 experience with terrorism prosecutions in many countries suggests that the tensions between the desire to keep intelligence secret and the requirements for disclosure have not gone away. In some respects, they may have intensified as prosecutors argue that it is more important than ever for them to satisfy disclosure obligations in order to obtain convictions, while security intelligence agencies argue that the need to keep their ongoing operations, methods and sources confidential has increased if they are to prevent another 9/11. Although the mandates of police and intelligence agencies have become more pressing since 9/11, there is a need to rethink these mandates in light of the need to prosecute and punish terrorists.

2. British Responses

Britain’s domestic Security Service, better known as MI5, provides a relevant example of how a security intelligence service can adjust its activities to better accommodate the need for evidence that can be used against suspected terrorists. Its official web site contains a section entitled “evidence and disclosure” which explains:

Security Service officers have been witnesses for the prosecution in a number of high profile criminal trials, and intelligence material has either been admitted in evidence or disclosed to the defence as “unused material” in a significant number of cases. This has occurred mostly in the context of our counter-terrorist and serious crime work.

⁶⁹ Report of the Joint Inquiry into the Terrorist Attacks of 9/11 by the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence December 2002 at 77.

⁷⁰ Report of the CIA Inspector General, June 2005 unclassified executive summary at xv at https://www.cia.gov/library/reports/Executive%20Summary_OIG%20Report.pdf

The increased involvement of the Service in criminal proceedings means that, when planning and carrying out intelligence investigations that may lead to a prosecution, we keep in mind the requirements of both the **law of evidence** and the **duty of disclosure**.

Our officers, working closely with members of law enforcement agencies, ensure that operations are properly co-ordinated with a view to the possible use of the resulting intelligence as evidence in court. For these reasons, as well as to ensure proper internal controls and compliance with legal obligations under the **Regulation of Investigatory Powers Act 2000 (RIPA)**, we keep detailed records of our operations, including all meetings with agents, eavesdropping, search and surveillance operations.

Judges have allowed staff to give evidence in criminal trials anonymously, including appearing behind screens. Arrangements correspond to those that have been made for undercover and specialist police officers and members of the special forces when giving evidence. The decision on these issues, however, rests with the judge in each case. Even where the judge makes an order for the screening and anonymity of Security Service witnesses, their evidence remains subject to cross-examination by the defence in the normal way.

As for relevant intelligence that is not used in evidence, the duty of prosecutors to disclose such “unused material” to the defence is set out in the **Criminal Procedure and Investigations Act 1996**. The Act does however recognise that the duty of disclosure must accommodate the need to protect sensitive information, the disclosure of which could damage important aspects of the public interest, such as national security.

Accordingly, where an investigation leads to a prosecution, prosecuting Counsel considers our records and advises which of them are disclosable to the defence. If disclosure would cause real damage to the public

interest by, for example, compromising the identity of an agent or a sensitive investigative technique, the prosecutor may apply to the judge for authority to withhold the material. Such applications take the form of a claim for **public interest immunity (PII)**.

Claims for PII in relation to our material are made on the basis of a certificate signed by the Home Secretary. In deciding whether a claim is appropriate, the Home Secretary carries out a careful balancing exercise between the competing public interests in the due administration of justice and the protection of national security. This exercise takes account of detailed advice from prosecuting Counsel on the relevance of the material to the issues in the case.

If the Home Secretary considers that the balance comes down in favour of non-disclosure, a claim for PII will be made. But the decision on a PII claim is one for the judge alone: it is the courts, not the Service or the Government, that ultimately decide what must be disclosed in a particular case. If a claim is accepted, the judge will continue to keep the decision under review throughout the proceedings.⁷¹

The Security Service Act, 1989 has been amended to make clear that information collected by MI5 in the proper discharge of its function can be “disclosed for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceeding”.⁷² A similar provision is also contained in the mandate of Britain’s foreign intelligence agency.⁷³ There are also provisions in the *Security Service Act, 1989* that provide that one of the functions of the Security Service is to act in support of police forces and other law enforcement agencies in the prevention and detection of serious crime and that require its Director to ensure that there are arrangements for co-ordinating the activities of the Security Service with police forces, the Serious Organized Crime Agency and other law enforcement agencies.⁷⁴ Although MI5 suspended its work on serious

⁷¹ MI5 “Evidence and Disclosure” at <http://www.mi5.gov.uk/output/Page87.html> (accessed Jan 21, 2007)

⁷² *Security Service Act, 1989* s.2(2)

⁷³ *Intelligence Services Act, 1994* s.2(2).

⁷⁴ *Security Service Act, 1989* ss.1(4), 2(2)(c).

crime such as drugs and arms trafficking in April, 2006 to concentrate on terrorism⁷⁵; its statutory mandate still facilitates co-ordination with the police and disclosure for the purpose of criminal proceedings.

Britain has codified common law standards of what information held by the Crown has to be disclosed to the accused so that they are considerably narrower than those that apply under *Stinchcombe* and apply only to information that could undermine the Crown's case or assist that of the accused. In addition, British terrorism prosecutions also feature requests by the Crown to the trial judge to order that intelligence not be disclosed to the accused on the basis of public interest immunity.⁷⁶ The former head of MI5 in a 2006 speech has commented that "Wherever possible we seek to collect evidence sufficient to secure prosecutions, but it is not always possible to do so: admissible evidence is not always available and the courts, rightly, look for a high standard of certainty. Often to protect public safety the police need to disrupt plots on the basis of intelligence but before evidence sufficient to bring criminal charges has been collected."⁷⁷ Dame Eliza Manningham-Buller has also recognized that intelligence can be "patchy and fragmentary and uncertain, to be interpreted and assessed. All too often it falls short of evidence to support criminal charges to bring an individual before the courts, the best solution if achievable. Moreover, as I said earlier, we need to protect fragile sources of intelligence including human sources".⁷⁸

The divide between intelligence and evidence in Britain is dynamic. There has been an increased willingness to admit intelligence in non-criminal proceedings, where it may never be disclosed to the directly affected party and only disclosed to a security-cleared special advocate.⁷⁹ The British experience suggests that both security intelligence agencies and the courts have adjusted their procedures to respond to the challenges of terrorism prosecutions which will involve some intelligence.

⁷⁵ MI5 "Serious Crime" at <http://www.mi5.gov.uk/output/Page52.html>

⁷⁶ See infra part 7 for a discussion of these matters

⁷⁷ Dame Eliza Manningham-Buller "The International Terrorist Threat to the United Kingdom", 2006 at <http://www.mi5.gov.uk/output/Page374.html>

⁷⁸ Dame Eliza Manningham-Buller "The International Terrorist Threat and the Dilemmas of Countering It", 2005 at <http://www.mi5.gov.uk/output/Page375.html>

⁷⁹ Clive Walker "Intelligence and Anti-Terrorism Legislation in the United Kingdom" (2005) 44 *Crime, Law and Social Change* 387.

3. Canadian Responses

i) The Anti-Terrorism Act

There have been many responses to 9/11 in Canada including an expansion of the budgets and the activities of both CSIS and CSE, the enactment of many new terrorism offences that apply to various forms of support, preparation and facilitation of terrorism, and the enactment of new regimes under the *Canada Evidence Act* to govern claims that material should not be disclosed on grounds of national security confidentiality. The *Canada Evidence Act* changes will be examined in detail in part six of the paper, but in essence they require the accused and other justice system participants to alert the Attorney General of Canada as soon as possible if they desire to use as evidence material broadly defined as sensitive and potentially injurious. The Attorney General can authorize the use of such information or challenge it before specially designated judges of the Federal Court, who will weigh the competing public interest in disclosure and non-disclosure. These judges have the ability to order disclosure, non-disclosure or partial disclosure, including the use of summaries. The trial judge is bound by non-disclosure orders, but can make any order required to protect the accused's right to a fair trial. The Attorney General can block a court order for disclosure with a certificate that can prohibit the disclosure of information relating to national security or defence or obtained from foreign entities for a fifteen-year period.

The creation of many new terrorism offences in the Criminal Code has implications for the relation between intelligence and evidence. The new offences include several offences relating to the financing of terrorism, including the provision or collection of property intending or knowing that it will be used for various forms of terrorism⁸⁰, making property or financial services available to benefit a terrorist group or intending or knowing that it will be used to facilitate terrorism,⁸¹ using or possessing property intending or knowing that it will be used to carry out or facilitate terrorism⁸², knowingly dealing or providing services in relation to terrorist property,⁸³ failing to disclose to the RCMP Commissioner and the CSIS Director property or transactions controlled by a terrorist group⁸⁴ and the failure of financial institutions to report on whether they

80 Criminal Code s.83.02

81 *ibid* s.83.03

82 *ibid* s.83.04

83 *ibid* s.83.08, 83.12

84 *ibid* ss.83.1, 83.12

possess or control property owned by a terrorist group.⁸⁵ In addition to these financing offences, six other new terrorism offences were added to the Code. These offences apply to participating in a terrorist group for the purpose of enhancing its ability to carry out terrorism⁸⁶, facilitating a terrorist activity regardless of whether a particular terrorist activity was planned or carried out⁸⁷, committing any indictable offence for the benefit, at the direction of or in association with a terrorist group,⁸⁸ instructing a person to carry out any activity for the purpose of enhancing the ability of a terrorist group to commit terrorism⁸⁹, instructing the carrying-out of a terrorist activity⁹⁰ and knowingly harbouring or concealing someone who has carried out or is likely to carry out a terrorist activity.⁹¹ The new Criminal Code amendments include broad definitions of a terrorist activity that includes attempts, conspiracies, counselling and threats to commit terrorist activities.

Other new crimes added to the Criminal Code by the *Anti-Terrorism Act* include threats against United Nations personnel, hate-motivated mischief relating to religious property and the placing of explosives in a public places. As with all crimes, conspiracies, attempts and counseling of these crimes could be prosecuted as separate offences before the actual crimes were committed. In addition, the *Official Secrets Act* was renamed and expanded in part to include passing on secret information to terrorist groups, asking persons to commit offences at the direction of terrorist groups or inducing persons by threat, accusation or menace to do anything that increases the capacity of a terrorist group to harm Canadian interests.

Although the precise ambit of the expansion of the criminal law is a matter of some debate, the 2001 *Anti-Terrorism Act* has criminalized a wide variety of conduct that occurs well before the actual commission of a terrorist act. The expansion of the criminal law means that what would have been, before 2001, advance intelligence that warns about threats to the security of Canada may, in some cases, now also be evidence of one of the new crimes outlined above.

The full implications of the *Anti-Terrorism Act* with respect to the relation between intelligence and evidence are only starting to become

⁸⁵ Ibid s.83.11, 83.12

⁸⁶ Ibid s.83.18

⁸⁷ Ibid s.83.19

⁸⁸ Ibid s.83.2

⁸⁹ Ibid s.83.21

⁹⁰ Ibid s.83.22

⁹¹ Ibid s.83.23

apparent. From 2001-2004, Canada relied on the use of immigration law security certificates to detain suspected terrorists. Until the Supreme Court's decision in *Charkaoui v. Canada*⁹², these certificates allowed the government to both keep its own and foreign intelligence secret and to present it before the designated judge of the Federal Court in an attempt to have the certificate and the detainee's detention upheld. No criminal charges were laid under the 2001 *Anti-Terrorism Act* until 2004 and the initial prosecution has been delayed by s.38 proceedings and appeals. A second terrorism prosecution in Canada remains at a preliminary stage. Canada has had much less experience with post 9/11 terrorism prosecutions compared with Australia, the United Kingdom and the United States.

ii. The Rae Report

In 2005, the Hon. Bob Rae, in his report on the Air India bombing, stressed the need to establish a workable and reliable relation between intelligence and evidence. He placed the relationship between intelligence and evidence into its larger political, historical and legal context by observing that:

The splitting off of security intelligence functions from the RCMP, and the creation of the new agency, CSIS, came just at the time that terrorism was mounting as a source of international concern. At the time of the split, counter-intelligence (as opposed to counter-terrorism) took up 80% of the resources of CSIS. The Cold War was very much alive, and the world of counter-intelligence and counter-espionage in the period after 1945 had created a culture of secrecy and only telling others on a "need to know" basis deeply pervaded the new agency.⁹³

He then went on to note some of the implications of 9/11:

The 9/11 Commission Report in the United States is full of examples of the difficulties posed to effective counter-terrorist strategies by the persistence of "stovepipes and firewalls" between police and security officials. Agencies were notoriously reluctant to share information, and were not able to co-operate sufficiently to disrupt

⁹² 2007 SCC 9

⁹³ Hon. Bob Rae *Lessons to be Learned* (2005) at 22-23

threats to national security. There is, unfortunately, little comfort in knowing that Canada has not been alone in its difficulties in this area. The issue to be faced here is whether anything was seriously wrong in the institutional relationship between CSIS and the RCMP, whether those issues have been correctly identified by both agencies, as well as the government, and whether the relationships today are such that we can say with confidence that our security and police operations can face any terrorist threats with a sense of confidence that co-operation and consultation are the order of the day.

The intelligence-evidence debate is equally important. If an agency believes that its mission does not include law enforcement, it should hardly be surprising that its agents do not believe they are in the business of collecting evidence for use in a trial. But this misses the point that in an age where terrorism and its ancillary activities are clearly crimes, the surveillance of potentially violent behaviour may ultimately be connected to law enforcement. Similarly, police officers are inevitably implicated in the collecting of information and intelligence that relate to the commission of a violent crime in the furtherance of a terrorist objective.⁹⁴

The Rae report poses the very important question of whether traditional attitudes towards secrecy and, indeed, some of the behaviour in the Air India investigation was rooted in a Cold War paradigm in which CSIS devoted 80% of its resources to counterintelligence efforts.

Although the Rae report focuses on the changed threat environment, it also notes that better management of the relation between intelligence and evidence can have due process benefits for those accused of terrorism. Rae notes that the failure to preserve CSIS tapes on Parmar could have harmed either the state's interest in crime control or the interest of the accused in due process. The tapes could have contained incriminating evidence that could be used in criminal prosecutions, but it is also possible that they could have contained exculpatory evidence. In any event, the destruction of the tapes, as well as CSIS interview notes, allowed the accused to argue that they were deprived of exculpatory evidence. It was

⁹⁴ *ibid*

only the 2005 acquittal that prevented Justice Josephson from having to craft a Charter remedy with respect to the Charter violations that he held occurred because of the destruction of the tapes and the interview notes. Rae commented that:

The erasure of the tapes is particularly problematic in light of the landmark decision of the Supreme Court of Canada in *R. v. Stinchcombe*, which held that the Crown has a responsibility to disclose all relevant evidence to the defence even if it has no plans to rely on such evidence at trial. Justice Josephson held that all remaining information in the possession of CSIS is subject to disclosure by the Crown in accordance with the standards set out in *Stinchcombe*. Accordingly, CSIS information should not have been withheld from the accused.⁹⁵

The Rae report usefully highlighted the need for further study of the relationship between evidence and intelligence in light of *Stinchcombe* and the new focus on counter-terrorism including the creation of many new crimes for preparation and support of terrorism.

iii. CSIS and the Conversion of Intelligence to Evidence

It is not clear whether CSIS and other security agencies have adjusted to the evidentiary implications of the expansion of the criminal law in relation to terrorism. In a speech given in March, 2002 Ward Elcock, then Director of CSIS, warned that most potential terrorists of interest to CSIS would not commit crimes and, even when they did, available evidence could not be used against them because of concerns about revealing a human source, classified technology or information obtained from foreign agencies. In his view, there was a need for an appropriate balance “between detection and forewarning and enforcement efforts”. He stressed the dangers of losing “all one’s intelligence assets and, therefore, any ability to monitor targets of concern down the road” for “a more minor criminal prosecution”.⁹⁶ At the same time, Mr. Elcock acknowledged that the 2001 *Anti-Terrorism Act*, especially in relation to new terrorism financing offences, “will allow law enforcement agencies to succeed in dealing with terrorist activities.”⁹⁷

⁹⁵ *ibid* at 16.

⁹⁶ *Ibid* at 35, 36.

⁹⁷ *ibid* at 36

In his 2003 John Tait Memorial Lecture, Ward Elcock elaborated on some of the differences he saw between law enforcement and security intelligence. He commented:

Law enforcement is generally reactive; it essentially takes place after the commission of a distinct criminal offence. Police officers are results-oriented, in the sense that they seek prosecution of wrong doers. They work on a “closed” system of limits defined by the Criminal Code, other statutes and the courts. Within that framework, they often tend to operate in a highly decentralized mode. Police construct a chain of evidence that is gathered and used to support criminal convictions in trials where witnesses are legally obliged to testify. Trials are public events that receive considerable publicity.

Security intelligence work is, by contrast, preventive and information-oriented. At its best, it occurs before violent events occur, in order to equip police and other authorities to deal with them. Information is gathered from people who are not compelled by law to divulge it. Intelligence officers have a much less clearly defined role, which works best in a highly centralized management structure. They are interested in the linkages and associations of people who may never commit a criminal act – people who consort with others who may be a direct threat to the interests of the state.

CSIS officers make no arrests, but call upon the police of jurisdiction if apprehension is required. Their work environment is an open-ended world of nuance and shades of meaning. Information is not collected as evidence at trial but as input to the decision-making centres of government. Management control is vital in this work so that individual investigators’ insights are frequently cross-checked by others, preventing personal bias from clouding the results. Finally, it is conducted in secret so that peoples’ identities and reputations are protected and in order to protect the policy options of the state.

Because of its open-ended, subtle and confidential nature, security intelligence work requires a close and thorough system of control and accountability in which political responsibility plays a large part.⁹⁸

These comments appear to be based on a dichotomy between reactive policing and proactive and secret intelligence. As discussed above, this dichotomy reflects conventional wisdom, originating with the 1983 Pitfield report, but it makes little allowance for the challenge of terrorism prosecutions as revealed by the Air India investigation or the post-9/11 experience.

The present head of CSIS, Jim Judd, has given speeches that stress the changed threat environment faced by Canada. He has commented that “the world of 1984 when CSIS was created is a different one from the one in which we live today. At the time of its establishment, we were in the midst of the Cold War and, not surprisingly, the focus of the organization was very much on foreign espionage activities in Canada. But time moves on and national security environments evolve.” In 2006, Mr. Judd described the differences between the mandate of CSIS and the police in the following terms:

While we work closely with the RCMP and other Canadian police services, law enforcement and intelligence are two very different activities. A variety of features differentiate the two,, including:

- CSIS is a civilian security intelligence agency, not a law enforcement agency – it has no powers of detention or capacity to compel cooperation and, of course, our personnel are not armed.
- Our objective is to investigate threats prior to action being taken or a crime committed while police more often than not devote more time, effort and resources to investigations of crimes after they have occurred.

⁹⁸ Ward Elcock “The John Tait Memorial Lecture” October, 2003 at http://www.csis.gc.ca/en/newsroom/speeches/speech17102003.asp?print_view=1

- As such, our principal objective is to collect intelligence and, where required, advise the Government of a potential threat. Unlike the police, we do not collect evidence per se (or collect information to evidentiary standards) to prosecute and secure convictions in court proceedings.
- CSIS has a lower threshold to undertake an investigation than do our police colleagues, ours being a “reasonable grounds to suspect” that certain activities constitute a threat to the security of Canada.
- Our mandate and authorities are set out in a single piece of legislation, enacted in 1984 and only very modestly amended five years ago in the omnibus 2001 anti-terrorism legislation.
- Our external review and oversight arrangements are different and, generally, more onerous than is the case with police services.⁹⁹

Although clearly recognizing the changed threat environment and with some differences in tone, Mr. Judd continued to conceptualize the police role as one that mainly reacts to crime. He affirmed the CSIS role as one that does not collect evidence or “collect information to evidentiary standards.”

In a speech given in April, 2008, Mr. Judd referred to “the judicialization of intelligence” in which intelligence was more involved in the legal process. He commented:

One of the consequences of recent trends in anti-terrorism actions has been a growing number of criminal prosecutions that have often had at their genesis, information collected by intelligence and not law enforcement agencies.

This in turn has increasingly drawn intelligence agencies in some jurisdictions into some interesting and important debates on a range of legal issues such as disclosure, evidentiary standards, and the testimony of intelligence personnel in criminal prosecutions.

⁹⁹ Notes for Remarks at the Royal Canadian Military Institute, Toronto, Sept. 28, 2006 at <http://www.csis-scrs.gc.ca/en/newsroom/speeches/speech28092006.asp>

While not startling or novel issues for the legal or police communities, these do have significant potential implications and consequences for the conduct of intelligence operations. In some instances, they have also stimulated some interesting debates over the boundary lines between law enforcement agencies and intelligence services.¹⁰⁰

Mr. Judd also observed that a variety of factors including legal proceedings were driving a debate about “what is legitimately secret and what is not” and that these changes “raise the issue as to whether or not existing legislative regimes are still current”.¹⁰¹

The idea that CSIS does not collect information to evidential standards has both defenders and critics. Although he is supportive of “sharing up” of information from the police to security intelligence agencies and recognizes the role of s.19 of the *CSIS Act* in authorizing “sharing down” from CSIS to the RCMP, Stanley Cohen, an experienced justice official and expert on privacy and criminal justice, has sounded several notes of caution about the use of intelligence in terrorism prosecutions. Cohen argues:

As a general proposition, national security concerns are inconsistent with a policy of full disclosure to law enforcement, (as a threshold matter, a proper security clearance is necessary in order to obtain and hold security information). The significance of an individual criminal investigation or charge may pale in comparison to the issues at stake in a complex national security operation. Disclosure in a given case may serve to endanger operatives or reveal their identities; or tend to reveal operational techniques that should be kept secret and safeguarded.

¹⁰⁰ Remarks at the Global Futures Conference, Vancouver, April 15, 2008 at <http://www.csis-scrs.gc.ca/nwsrm/spchs/spch15042008-eng.asp>

¹⁰¹ Ibid.

Disclosures of sensitive information may potentially compromise an ongoing investigation.¹⁰²

Cohen also expresses concerns about the privacy implications of increasing the transfer of information from security intelligence agencies to the police because “an intelligence dossier will naturally contain a range of information, including much that is unsifted or unfiltered, as well as innuendo, hearsay and speculation.” Intelligence in police hands, he suggests, could lead “to dossier building and the creation of generalized suspect lists.”¹⁰³ The examples of legitimate information sharing from CSIS to the RCMP cited by Cohen involve not the broad range of new terrorism offences, but other matters such as “ordinary criminal frauds, tax evasions, regulatory contraventions and so on...”¹⁰⁴ As will be seen, the findings of the Arar Commission support many of Cohen’s concerns about the misuse of intelligence in the hands of the police. Cohen concludes that CSIS “cannot and should not become a stalking horse or proxy for law enforcement.”¹⁰⁵

Marlys Edwardh, an experienced criminal defence lawyer, who acted in terrorism prosecutions in the 1980’s, as well as for Mr. Arar, has argued that CSIS should in some circumstances gather its intelligence to evidentiary standards. She suggests that CSIS has not learned the appropriate lessons from the Air India investigation, where it destroyed wiretaps and notes and tape recordings of crucial witness interviews. She concludes:

CSIS policies have not changed. Two illustrations of the damage that results from this stubborn persistence will suffice. The first involves the case of Bhupinder Singh Liddar.... The [SIRC] report claimed that CSIS investigators routinely destroy screening interview notes and that

¹⁰² Stanley Cohen *Privacy, Crime and Terror Legal Rights and Security in a Time of Peril* (Toronto: LexisNexis, 2005) at 403. Other factors cited by Cohen include: “the fact that the disclosure of subject information may ultimately become public in an open proceeding, such as a criminal trial; the downstream implications of revealing information that may ultimately tend to reveal covert, secret or surreptitious operational practices and techniques; the need to protect sensitive sources and the requirement to adhere to agreements and undertakings with other nations in the interest of securing the nation’s security and of promoting international cooperation and comity with Canada’s friends and allies in the international community. In addition, substantial encumbrances involving the initial acquisition of the information in question may exist that may delimit or constrain its subsequent use.” Ibid at 408.

¹⁰³ Ibid at 404.

¹⁰⁴ Ibid at 408. He cites a hostage taking as another example. Ibid at 406.

¹⁰⁵ Ibid at 407.

CSIS will lie and manipulate information to achieve its ends. The second example is the case of Adil Charkaoui... Charkaoui was interviewed by CSIS and the transcripts of the interview were destroyed after CSIS summarized the interviews in accordance with CSIS policy. ... The interviews took place in early 2002 – this demonstrates that the CSIS policy of evidence destruction remained in place 10 years after the SIRC 'Air India' admonition.¹⁰⁶

The Supreme Court's decision in the *Charkaoui* case described above which involves destruction of CSIS notes is pending. The concerns raised by Edwardh are essentially that CSIS has not respected the due process implications of its collection of information. As the Rae report reveals, however, there are both due process and crime control consequences when CSIS does not recognize the evidentiary implications of its work in the counter-terrorism area.

iv. The Arar Commission

The Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar also examined distinctions between security intelligence and law enforcement. The Arar Commission found no fault with the decision of CSIS to hand over a series of individuals, in the immediate aftermath of 9/11, for investigation by the RCMP in the A-0 Canada investigation. Justice O'Connor stated that it was "wrong" to interpret the McDonald Commission and related reforms as "indicating that the RCMP should not be involved in any national security activities whatsoever." Although the mandates of CSIS and the RCMP are different, they also:

...contemplate a continuum in the collection of information concerning national security threats. CSIS collects information at an earlier phase and on a broader basis than does the RCMP. It collects information and/or intelligence under section 12 of the *CSIS Act* in respect of activities that may on reasonable grounds be suspected of constituting threats to the security of Canada' and advises government of perceived threats to the security of Canada. CSIS is not a law enforcement agency, and

¹⁰⁶ Marlys Edwardh "Problems of Proof in Terrorist Offences", 2006 prepared for National Criminal Law Program

once it makes a determination that sufficient indicators of criminality are present to warrant a criminal investigation, the RCMP may become involved...

In addition to conducting criminal investigations for purposes of prosecution, the RCMP has a preventive mandate under section 18 of the RCMP Act which gives it authority to conduct investigations aimed at taking steps to preserve the peace and prevent crimes.

Although some have suggested that 9/11 inappropriately thrust the RCMP back into the national security business, contrary to the direction of the McDonald Commission, that is not the case. The RCMP has conducted investigations with national security implications in the years since the McDonald Commission... What has changed since 9/11 is the number and intensity of the RCMP's national security investigations and the enactment of Bill C-36 which, among other things, created new criminal offences relating to national security, as well as certain new investigative powers. In the months and years since 9/11, the RCMP has devoted a significantly larger proportion of its resources to these types of investigations, and it would seem that this higher level of activity will continue to be required for the foreseeable future.¹⁰⁷

The very first recommendation made by Justice O'Connor was that "the RCMP should take active steps to ensure that it stays within its mandate as a police force to perform the duties of peace officers in preventing and prosecuting crime" and that it should respect "the distinct role of CSIS in collecting and analyzing information and intelligence relating to threats to the security of Canada."¹⁰⁸ Although acknowledging the need for increased co-operation and information-sharing between the RCMP and CSIS, Justice O'Connor concluded that the basic principle surrounding the separation of the security intelligence from the law enforcement function was sound.

¹⁰⁷ Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar *Analysis and Recommendations* (Ottawa: Supply and Services, 2006) at 67-68.

¹⁰⁸ *Ibid* at 312.

The Arar Commission criticized the A-O Canada RCMP investigation for failing to place restrictions or caveats on the use of information that it shared with American officials and for failing to respect restrictions on further sharing of information that it received from other agencies. It stressed the importance of both restricting the use of information that is shared, and respecting the caveats that other agencies have placed on information. Justice O'Connor observed:

Despite this need, some RCMP officers testified that, because of the imminent threat of another terrorist attack following 9/11, it had no longer been practical or desirable at the time to adhere to policies on screening information using caveats for information shared with the United States. As some expressed it, 'caveats were down'¹⁰⁹

Justice O'Connor agreed with senior RCMP officers that such an approach was not necessary even in the aftermath of 9/11. He stated:

It is wrong to think that caveats must 'be down', to use the expression of several witnesses at the Inquiry, in order for information to be shared effectively and efficiently. Caveats should not be seen as a barrier to information sharing, especially information sharing beyond that contemplated on their face. They can easily provide a clear procedure for seeking amendments or the relaxation of restrictions on the use and further dissemination of information in appropriate cases. This procedure need not be time-consuming or complicated. With the benefit of modern communications and centralized oversight of information sharing within the RCMP, requests from recipients should be able to be addressed in an expeditious and efficient manner.¹¹⁰

Although the Arar Commission stressed the importance of caveats which restricted the subsequent use of information, it did not conceive of caveats as impenetrable barriers to the evidentiary use of intelligence. Rather, it concluded that the proper approach would be to request the originator of the information to amend the caveat to permit the use of the information in subsequent proceedings. In some cases, the originator might refuse to amend the caveats, but in other cases the caveat could be amended to

¹⁰⁹ *ibid* at 108.

¹¹⁰ *ibid* at 339.

allow intelligence to be used as evidence, even though such uses were originally and routinely restricted.

The Arar Commission recognized some important changes in the legal and policy environment since 9/11 that have implications for the relation between evidence and intelligence. One important change was the enactment of the *Anti-Terrorism Act* that had the effect of enlarging the crime based mandate of the RCMP. In this respect, Justice O'Connor stated:

It would be wrong, however, to conclude that respecting its institutional mandate requires the RCMP to wait until an act of terrorism has occurred before taking action. The RCMP's mandate includes preventing crime, not just investigating it after the fact. Moreover, many crimes related to terrorism are committed long before a terrorist act causes actual harm. The RCMP's mandate has always included investigating conspiracies, attempts and counselling of serious crimes. Since the enactment of the *Anti-terrorism Act*, it has also entailed investigating a broad range of acts relating to potential terrorist activities, such as the financing and counselling of terrorism, participation in terrorist groups, and related attempts, conspiracies, and threats.¹¹¹

Although it rejected the idea that the RCMP was ever excluded from national security investigations, the Arar Commission noted the important changes of the *Anti-Terrorism Act* and how it increased the evidentiary significance of intelligence.

Another change noted by the Arar Commission was the development of "intelligence-led policing" since the early 1990's, when the RCMP recognized that its "failure to develop a sophisticated strategic as well as tactical intelligence capability" had "seriously hindered the Force's ability to accurately measure and prevent crime having an organized, serious or national security dimension in Canada, or internationally as it affects Canada."¹¹² It recognized that:

¹¹¹ *ibid* at 313.

¹¹² RCMP's 1991 Criminal Intelligence Program Implementation Guide as quoted Commission of Inquiry in the Actions of Canadian Officials in Relation to Maher Arar *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Supply and Services, 2006) at 43.

in the national security context, the very same information can be both criminal intelligence and security intelligence. It is also clear that both forms of intelligence can be gathered and analyzed in the same way. In addition while 'criminal intelligence' is collected to further the RCMP's criminal mandate, the link between the collection of intelligence and a criminal prosecution can be somewhat distant.¹¹³

The Commission recommended the continuation of intelligence-led policing, but with appropriate measures to ensure that it remained within the RCMP's law enforcement mandate and expertise and subject to enhanced review.

In addition, the Arar Commission documented fundamental changes in the organizational structure of national security policing in the RCMP. These changes were designed to make such policing much more centralized and better integrated with other agencies, including CSIS. These wide reaching changes included Ministerial directives issued in November, 2003, that were designed to increase centralization of the RCMP's national security investigations in order to enhance the Commissioner's operational accountability and Ministerial knowledge and accountability for high profile or controversial national security investigations. A Director General of National Security was also created in 2003 in RCMP headquarters in Ottawa, with responsibility for providing centralized approval and oversight of RCMP national security investigations. In addition, Integrated National Security Enforcement Teams (INSETS) have been created in Vancouver, Ottawa, Toronto and Montreal and include representatives of CSIS as well as representatives of other policing forces.

In its second report, the Arar Commission documented increased integration in national security activity that saw the RCMP working more closely with CSIS, a new Integrated Threat Assessment Centre, the CSE, Canadian Border Services Agency, Citizenship and Immigration Canada, the Financial Transactions Reports Analysis Centre (FINTRAC) and the Department of Foreign Affairs, among other agencies. Because of increased integration and information sharing, the Arar Commission recommended enhanced review of these agencies, including possibilities of joint and integrated review in order to mirror joint and integrated

¹¹³ *ibid* at 43.

national security activities. Although the Arar Commission did not focus on the relation between intelligence and evidence, it made findings about integration and information sharing that are consistent with an increased likelihood that intelligence collected by various domestic and foreign agencies could have an evidentiary use in national security criminal investigations or be subject to disclosure as relevant information possessed by the Crown.

v. The 2006 RCMP/CSIS MOU

A new Memorandum of Agreement signed between the Commissioner of the RCMP and the Director of CSIS in September, 2006 recognizes some of the changes outlined above. It addresses the relation between intelligence produced by CSIS and evidence that may be disclosed to the accused and used at criminal trials in a more thorough way than previous MOUs. Article 21 of the 2006 MOU provides:

The CSIS and the RCMP recognize that information and intelligence provided by the CSIS to the RCMP may have potential value as evidence in the investigation or prosecution of a criminal offence. In these cases, the parties will be guided by the following principles:

- a) both parties recognize that the CSIS does not normally collect information or intelligence for evidentiary purposes;
- b) both parties recognize that once information or intelligence has been disclosed by the CSIS to the RCMP, it may be deemed for purposes of the prosecution process to be in the control and possession of the RCMP and the Crown and thereby subject to the laws of disclosure whether or not the information is actually used by the Crown as evidence in court proceedings;
- c) Sections of the *Canada Evidence Act* will be invoked as required to protect national security information and intelligence.¹¹⁴

This new MOU recognizes that information and intelligence collected by CSIS “may have potential value as evidence in the investigation or prosecution of a criminal offence.” As suggested above, the many new

¹¹⁴ 2006 RCMP-CSIS MOU public production no. 1374.

crimes in the 2001 *Anti-Terrorism Act* means that more CSIS information collected in counter-terrorism investigations may have evidentiary value.

The new MOU also recognizes that one of the consequences of information sharing from CSIS to the RCMP is that the information, once it is in the control of the RCMP and the Crown, may have to be disclosed to the accused. This reflects the importance of the *Stinchcombe* disclosure obligations. Finally, the new MOU recognizes the ability of the Attorney General of Canada to use the enhanced provisions of the *Canada Evidence Act* to protect national security and intelligence from disclosure. As will be discussed below, these powers include not only the ability to make *ex parte* submissions to the Federal Court about the dangers of disclosure, but also to counter court-ordered disclosure with an Attorney General's certificate that will prohibit all disclosure of information relating to national defence or national security or obtained from foreign sources for a fifteen year period. The MOU indicates a growing awareness of the close connection between intelligence and terrorism in the post 9/11 era. At the same time, however, invocation of the enhanced provisions in s.38 of the CEA is not a panacea. As will be seen in subsequent sections, they fragment and prolong criminal trials.

I) Summary

Although the RCMP and CSIS retain and should respect their different mandates, they operate in a dynamic legal and policy environment. The crime prevention and evidence collection mandate of the RCMP has been increased with the enactment of the 2001 ATA. This law contains many new terrorism offences that will be complete long before any act of terrorism. The RCMP has also recognized that terrorism investigations must be more centralized than other police investigations; that they must be informed by intelligence; and that they must involve more co-operation with a wide variety of other actors, including CSIS. Security intelligence agencies may more frequently possess information that could be useful in criminal investigations and prosecutions, especially under the ATA.

The above developments suggest a need to re-think stark dichotomies between reactive policing and proactive intelligence; between decentralized policing and centralized intelligence and between secret intelligence and public evidence. All of these dichotomies are based on

the prevailing attitude at the time CSIS was created in 1984 during the Cold War, even though a close reading of the *CSIS Act* and *Security Offences Act* reveals a recognition that intelligence may have to be passed onto to the police when relevant to a police investigation and prosecution. The 1985 Air India bombings producing 331 deaths should have shattered simplistic dichotomies between secret intelligence and public evidence. Nevertheless, they persisted for some time and played a role in tensions between the RCMP and CSIS. In any event, the events of 9/11, and the passage of the 2001 ATA, should result in a thorough re-evaluation of the relation between intelligence and evidence.

Intelligence about terrorism can be relevant to possible criminal investigations into a wide range of serious criminal offences involving various forms of support, association and participation in terrorism and terrorist groups. Many of these investigations focus on associations and activities of targets and persons of interest. Such intelligence can be valuable to accused persons in defending themselves against allegations of support for and participation in terrorism. Although the need to protect sources, methods, ongoing investigations and foreign intelligence remains important, these demands should be re-thought in light of the need to prosecute and punish terrorists. Security intelligence agencies may have to become better acquainted with witness protection programs that are used in the criminal justice system and with the demands of the collection of evidence. In this respect, it is noteworthy that MI5 accepts the need to collect some evidence (albeit not electronic surveillance which is still generally inadmissible in British courts) to an evidentiary standard. Requests may have to be made to foreign agencies to consent to the disclosure of some information for the purposes of criminal prosecutions. Foreign countries are also dealing with the demands of terrorism prosecutions and may be willing to consider reasonable requests to allow the disclosure of some intelligence that they have provided to Canada. The world has changed since the original creation of the *CSIS Act*. There is a need for some new and creative thinking that challenges conventional wisdom in order to ensure a workable relationship between intelligence and evidence.

II. Fundamental Principles Concerning Intelligence and Evidence

The following four principles are broadly consistent with the seven principles identified by Bruce MacFarlane in his companion study on structural aspects of the criminal trial. In other words, the principles articulated here encompass the values of respect for the rule of the law

and the Charter including the rights of the accused and the right of the public to open trials and to the efficient and accurate pursuit of the truth in criminal trials, including the need to prevent wrongful convictions.¹¹⁵ At the same time, the principle of the need to keep secrets is particularly important to the relation between intelligence and evidence which is the focus of this study.

A) The Need to Keep Secrets

The disclosure of intelligence to the accused and the public can have serious adverse effects on ongoing investigations, security operations and ultimately to the ability of security agencies to help prevent acts of terrorism. Disclosure of secrets could also expose a confidential source to harm, including torture or death.

The Supreme Court, in upholding mandatory provisions for *ex parte* and *in camera* proceedings under the *Access to Information Act* in cases where foreign confidences or national security exemptions were claimed, stressed the need for Canada to maintain the confidences of its allies that information and intelligence that they shared with Canada would remain confidential. Arbour J. stated for the Court:

The mandatory *ex parte in camera* provision is designed to avoid the perception by Canada's allies and intelligence sources that an inadvertent disclosure of information might occur, which would in turn jeopardize the level of access to information that foreign sources would be willing to provide. In her reasons, Simpson J. reviewed five affidavits filed by the respondent from CSIS, the RCMP, the Department of National Defence ("DND"), and two from the Department of External Affairs ("DEA"). These affidavits emphasize that Canada is a net importer of information and the information received is necessary for the security and defence of Canada and its allies. The affidavits further emphasize that the information providers are aware of Canada's access to information legislation. If the mandatory provisions were relaxed, all predict that this would negatively affect the flow and

¹¹⁵ The seven principles outlined by Bruce MacFarlane in "Structural Aspects of Terrorist Trials" are 1) the pursuit of truth 2) public confidence and perceived legitimacy of proceedings, 3) fairness and the rule of law, 4) efficiency, 5) openness and publicity of criminal proceedings, 6) balancing individual rights with the public interests and 7) minimizing the risks of convicting the innocent.

quality of such information. This extract from one of the affidavits from the DEA is typical:

Canada is not a great power. It does not have the information gathering and assessment capabilities of, for instance, the United States, the United Kingdom or France. Canada does not have the same quantity or quality of information to offer in exchange for the information received from the countries which are our most important sources. If the confidence of these partners in our ability to protect information is diminished, the fact that we are a relatively less important source of information increases our vulnerability to having our access to sensitive information cut off.¹¹⁶

The Court's decision in *Ruby v. Canada* to uphold mandatory *ex parte* procedures under access to information legislation was undoubtedly influenced by the context of the case which did not involve a criminal prosecution or other deprivation of liberty.

In the different context of security certificates used to detain and deport non-citizens, the Supreme Court was more troubled by mandatory provisions giving the state the right to make *ex parte* submissions to the judge. Although it held that *ex parte* proceedings in security certificates under immigration law constituted an unjustified violation of s.7 of the Charter in *Charkaoui v. Canada*¹¹⁷, the Supreme Court readily recognized under s.1 of the Charter that:

The protection of Canada's national security and related intelligence sources undoubtedly constitutes a pressing and substantial objective. Moreover, the *IRPA*'s provisions regarding the non-disclosure of evidence at certificate hearings are rationally connected to this objective. The facts on this point are undisputed. Canada is a net importer of security information. This information is essential to the security and defence of Canada, and disclosure would adversely affect its flow and quality: see *Ruby*. This leaves the question whether the means Parliament has chosen, i.e. a certificate procedure

¹¹⁶ *ibid* at para 44-45

¹¹⁷ 2007 SCC 9

leading to detention and deportation of non-citizens on the ground that they pose a threat to Canada's security, minimally impairs the rights of non-citizens.¹¹⁸

In both *Ruby* and *Charkaoui*, the Supreme Court recognized the importance of the secrecy of the foreign intelligence that Canada receives from its allies and Canada's particular position as a net importer of intelligence. In addition, both the 9/11 Commission and the Arar Commission have affirmed the importance of information sharing among and between governments. Such information sharing often depends upon expectations that the information that is shared will be kept secret.

The importance of protecting secret information that, if disclosed, might harm national security is also underlined in a number of other legal instruments. One is the *Security of Information Act* which provides for a series of serious crimes with respect to the divulging of secret information. One part of this Act has recently been struck down as unconstitutional, but the trial judge recognized that the purpose of punishing and deterring the release of certain government information was pressing and substantial, and had been "reinforced...in the uncertain national security climate after the terrorist attacks of 2001".¹¹⁹

Another relevant legal instrument, which will be examined more fully below, is s.38 of the *Canada Evidence Act* which places requirements on all participants in the justice system to notify the Attorney General with respect to the disclosure of information that could injure international relations, national defence or national security.¹²⁰ The importance of protecting national security information is also underlined by s.38.13 of the *Canada Evidence Act*, which enables the Attorney General of Canada to prohibit even court-ordered disclosure of information relating to national defence or security or obtained from a foreign entity.¹²¹ This represents an ultimate vehicle to protect the state's interests and commitments to other states to keep secrets. At the same time, the value of secrecy is not absolute, as s.38.14 recognizes the right of the criminal trial judge to order whatever remedy is required in light of non-disclosure orders in order to protect the fairness of the accused's trial.

¹¹⁸ *ibid* at para 68

¹¹⁹ *O'Neill v. Canada* (2006) 82 O.R.(3d) 241 at paras 95 -96 (Ont. Sup.Ct.)

¹²⁰ CEA s.38.01

¹²¹ *ibid* s.38.13

Even outside the national security and international relations context, the Court has recognized the importance of protecting confidential sources, both in terms of ensuring their own safety and in terms of ensuring that people continue to provide information to the state. In *R. v. Leipert*¹²², the Supreme Court held that the police need not disclose the identity of an informer who provided an anonymous crime stopper tip that led them to investigate a person for growing marijuana. It rejected the accused's argument that he was entitled, under the disclosure requirements of *Stinchcombe*, to the sheet used to collect the tip, albeit edited in a manner to protect the informer's identity. Noting both the need to protect the informer's safety and to encourage others to share information with the police, the Court concluded that "informer privilege is of such importance that it cannot be balanced against other interests. Once established, neither the police nor the court possesses discretion to abridge it."¹²³ The Court also held that the trial judge had erred in disclosing an edited tip sheet to the accused because of the dangers of inadvertently revealing information to the accused that could allow the informer to be identified.¹²⁴ The Court rejected the argument that the informer privilege was inconsistent with *Stinchcombe* disclosure obligations on the basis that the disclosure rules were themselves subject to evidentiary privileges, including the informer privilege. The informer privilege is a hallowed privilege that is subject only to an innocence at stake exception. Even if that limited exception applies, "the State then generally provides for the protection of the informer through various safety programs, again illustrating the public importance of that privilege."¹²⁵

The importance of the informer privilege was recently affirmed in *Named Person v. Vancouver Sun*.¹²⁶ The Court stressed that the privilege applied to all information that might identify an informer and that it was a non-discretionary legal right that belonged to both the informer and the Crown.

In conclusion, the general rationale for the informer privilege rule requires a privilege which is extremely broad and powerful. Once a trial judge is satisfied that

¹²² [1997] 1 S.C.R. 287

¹²³ Ibid at para 14.

¹²⁴ "A detail as innocuous as the time of the telephone call may be sufficient to permit identification. In such circumstances, courts must exercise great care not to unwittingly deprive informers of the privilege which the law accords to them." Ibid at para 16.

¹²⁵ *R. v. McClure* [2001] 1 S.C.R. 445 at para 45.

¹²⁶ 2007 SCC 43

the privilege exists, a complete and total bar on any disclosure of the informer's identity applies. Outside the innocence at stake exception, the rule's protection is absolute. No case-by-case weighing of the justification for the privilege is permitted. All information which might tend to identify the informer is protected by the privilege, and neither the Crown nor the court has any discretion to disclose this information in any proceeding, at any time.¹²⁷

The Court indicated that when an informer seeks the benefit of the privilege the judge should hold *in camera* proceedings with only the informer and the Attorney General present to determine whether the privilege applies. Third parties such as the media have no role to play in determining whether the privilege exists, but they may have a role in determining the extent of the information that can be released.

The importance of protecting national security information and confidential informers is well recognized in Canadian law. The law provides the government with many strong tools to protect secret information from disclosure.

B) The Need to Treat the Accused Fairly

The need to treat the accused fairly and to ensure that there is a fair trial is the bedrock principle of fundamental justice. The importance of adjudicative fairness was affirmed in *Charkaoui v. Canada*,¹²⁸ in the course of holding that mandatory *ex parte* provision of secret evidence which could be used against a detainee under an immigration security certificate was an unjustified violation of s.7 of the Charter. The Court made clear that while some adjustments could be made because of the need to protect secrets and other national security concerns, at the end of the day any remaining procedure must be fundamentally fair. Chief Justice McLachlin explained:

while administrative constraints associated with the context of national security may inform the analysis on whether a particular process is fundamentally unfair, security concerns cannot be used to excuse procedures that do not conform to fundamental justice at the s. 7

¹²⁷ *ibid* at para 30.

¹²⁸ 2007 SCC 9

stage of the analysis. If the context makes it impossible to adhere to the principles of fundamental justice in their usual form, adequate substitutes may be found. But the principles must be respected to pass the hurdle of s. 7. That is the bottom line.

The procedures required to conform to the principles of fundamental justice must reflect the exigencies of the security context. Yet they cannot be permitted to erode the essence of s. 7. The principles of fundamental justice cannot be reduced to the point where they cease to provide the protection of due process that lies at the heart of s. 7 of the *Charter*. The protection may not be as complete as in a case where national security constraints do not operate. But to satisfy s. 7, meaningful and substantial protection there must be.¹²⁹

In *Charkaoui*, the Court affirmed that “a fair hearing requires that the affected person be informed of the case against him or her, and be permitted to respond to that case.”¹³⁰ Although the Court held that designated judges reviewing security certificates remained independent and impartial, it concluded that the use of secret information not disclosed to the detainee or subject to adversarial cross examination was unconstitutional. It deprived the detainee of “an opportunity to meet the case put against him or her by being informed of that case and being allowed to question or counter it.” The Court concluded that:

Fundamental justice requires substantial compliance with the venerated principle that a person whose liberty is in jeopardy must be given an opportunity to know the case to meet, and an opportunity to meet the case. Yet the imperative of the protection of society may preclude this. Information may be obtained from other countries or from informers on condition that it not be disclosed. Or it may simply be so critical that it cannot be disclosed without risking public security. This is a reality of our modern world. If s. 7 is to be satisfied, either the person must be given the necessary information, or a substantial substitute for that information must be found. Neither is the case here.¹³¹

¹²⁹ *ibid* at paras 23 and 27.

¹³⁰ *ibid* at para 53.

¹³¹ *ibid* at para 61.

Section 7 allows for a certain amount of flexibility and creativity to reconcile the demands of secrecy and fairness, but “the bottom line” is that the process must be fair.

Even after concluding that the procedures violated the basic requirements under s.7 of the Charter, the Court considered whether the government had justified the limitation of the detainee’s rights under s.1 of the Charter. It examined a wide range of alternative mechanisms to reconcile fairness with secrecy. They included the use of security-cleared special advocates or security-cleared counsel, employed by SIRC and the Arar Commission, to test and challenge the intelligence presented to justify detention under a security certificate. The Court also noted:

Crown and defence counsel in the recent *Air India* trial (*R. v. Malik*, [2005] B.C.J. No. 521 (QL), 2005 BCSC 350) were faced with the task of managing security and intelligence information and attempting to protect procedural fairness. The Crown was in possession of the fruits of a 17-year-long investigation into the terrorist bombing of a passenger aircraft and a related explosion in Narita, Japan. It withheld material on the basis of relevance, national security privilege and litigation privilege. Crown and defence counsel came to an agreement under which defence counsel obtained consents from their clients to conduct a preliminary review of the withheld material, on written undertakings not to disclose the material to anyone, including the client. Disclosure in a specific trial, to a select group of counsel on undertakings, may not provide a working model for general deportation legislation that must deal with a wide variety of counsel in a host of cases. Nevertheless, the procedures adopted in the *Air India* trial suggest that a search should be made for a less intrusive solution than the one found in the *IRPA*¹³²

The Court’s survey of less rights intrusive alternatives in *Charkaoui* demonstrates its willingness both under s.7 and s.1 of the Charter to make accommodations for the need to keep secrets while at the same time ensuring that basic fairness is achieved.¹³³

¹³² *ibid* at para 78.

¹³³ *ibid* at para 139.

Although *Charkaoui* is a recent and important case on reconciling fairness and secrecy, and it involved long-term detention and restrictions of liberty under immigration law security certificates, allowance must also be made for the particular focus of criminal prosecutions. The Court's discussion of alternative methods of reconciling fairness and secrecy in *Charkaoui* implicitly acknowledges the distinctiveness of the criminal trial process in its discussion of s.38 of the CEA as an alternative. The Court commented:

Under the recent amendments to the CEA set out in the *Anti-terrorism Act*, S.C. 2001, c. 41, a participant in a proceeding who is required to disclose or expects to disclose potentially injurious or sensitive information, or who believes that such information might be disclosed, must notify the Attorney General about the potential disclosure, and the Attorney General may then apply to the Federal Court for an order prohibiting the disclosure of the information: ss. 38.01, 38.02, 38.04. The judge enjoys considerable discretion in deciding whether the information should be disclosed. If the judge concludes that disclosure of the information would be injurious to international relations, national defence or national security, but that the public interest in disclosure outweighs in importance the public interest in non-disclosure, the judge may order the disclosure of all or part of the information, on such conditions as he or she sees fit. No similar residual discretion exists under the *IRPA*, which requires judges not to disclose information the disclosure of which would be injurious to national security or to the safety of any person. Moreover, the CEA makes no provision for the use of information that has not been disclosed. While the CEA does not address the same problems as the *IRPA*, and hence is of limited assistance here, it illustrates Parliament's concern under other legislation for striking a sensitive balance between the need for protection of confidential information and the rights of the individual.

The criminal trial process is distinct from immigration law in several respects. One is that the criminal trial judge has an explicitly recognized discretion under s.38.14 of the CEA to order whatever remedy is appropriate, including a stay of proceedings, to protect the accused's

right to a fair trial. A second difference is that s.38.06 of the CEA allows the judge to order disclosure of information that would harm national security, but on the basis that the public interest in disclosure is greater. Finally, s.38 of the CEA only provides a means for the state to obtain non-disclosure orders; it does not contemplate the use of secret evidence in criminal trials.

Although secret evidence that is not disclosed to the accused will not be used in criminal trials, it would be a mistake to conclude that dilemmas in reconciling secrecy and fairness will not affect criminal trials. The Courts have in a number of criminal cases been sensitive to placing the accused in an impossible, or “catch 22”, situation in which he or she has to establish the content or relevance of documents without having access to them. In *R. v. Garofoli*,¹³⁴ the Court affirmed the importance of opening sealed packages to allow the accused to exercise the right to full answer and defence in order to challenge the authorization for the warrant. In *R. v. Mills*,¹³⁵ the Court again stressed the importance of the accused’s right to full answer and defence:

Our jurisprudence has recognized on several occasions “the danger of placing the accused in a ‘Catch-22’ situation as a condition of making full answer and defence”: *O’Connor, supra*, at para. 25; see also *Dersch, supra*, at pp. 1513-14; *R. v. Garofoli*, [1990] 2 S.C.R. 1421, at pp. 1463-64; *Carey v. Ontario*, [1986] 2 S.C.R. 637; *R. v. Durette*, [1994] 1 S.C.R. 469. This is an important consideration in the context of records production as often the accused may be in the difficult position of making submissions regarding the importance to full answer and defence of records that he or she has not seen. Where the records are part of the case to meet, this concern is particularly acute as such a situation very directly implicates the accused’s ability to raise a doubt concerning his or her innocence.... Where the records to which the accused seeks access are not part of the case to meet, however, privacy and equality considerations may require that it be more difficult for accused persons to gain access to therapeutic or other records.....

¹³⁴ [1990] 2 S.C.R. 1421.

¹³⁵ [1999] 3 S.C.R. 668.

Several principles regarding the right to make full answer and defence emerge from the preceding discussion. First, the right to make full answer and defence is crucial to ensuring that the innocent are not convicted. To that end, courts must consider the danger of placing the accused in a Catch-22 situation as a condition of making full answer and defence, and will even override competing considerations in order to protect the right to make full answer and defence in certain circumstances, such as the “innocence at stake” exception to informer privilege. Second, the accused’s right must be defined in a context that includes other principles of fundamental justice and *Charter* provisions. Third, full answer and defence does not include the right to evidence that would distort the search for truth inherent in the trial process.¹³⁶

In the above case, the Supreme Court upheld legislative restrictions on both the disclosure of private documents held by the Crown and the production of private documents held by third parties in sexual assault cases. This indicates that the accused’s right to production and disclosure is not absolute, but also that the courts will not readily accept non-disclosure or non-production of material that adversely affects the accused’s ability to meet the case and his or her right to full answer and defence.

Not all of the dilemmas of reconciling fairness and secrecy in criminal trials will stem from requests by the accused for disclosure of documents that he or she has not seen. Questions of fairness may arise when non or partial disclosure orders are made under s.38 of the CEA, and the criminal trial judge has to decide whether a fair trial is possible in light of a non-disclosure order or a partial disclosure order, such as the use of summaries. Another possible dilemma is when the accused wants to call witnesses to give evidence in his or her defence, but the evidence and perhaps even the identity of the potential witness is subject to a national security confidentiality claim. All of these dilemmas can emerge at a criminal trial and they can place the fairness of the criminal trial in jeopardy.

In the last section, we examined the high priority that traditionally has been given to the protection of an informer’s identity and how the Supreme

¹³⁶ *ibid* at paras 71, 76.

Court has exempted information subject to informer privilege from the *Stinchcombe* duty of disclosure. That said, however, the protection of informers is not absolute and is subject to the accused's right to full answer and defence in at least two respects. In *R. v. Leipert*, the Court held that the confidential informant to the crime stopper program could be protected but that, in fairness to the accused, the search warrant would have to be defended by the state without reliance on the informer's information.¹³⁷ Evidence that could not be disclosed to the accused could not be used against him. Fairness and secrecy could be reconciled by allowing the state to attempt to defend the warrant, minus the information that could not be disclosed to the accused. As will be seen, a similar approach has been taken in some important terrorism prosecutions.¹³⁸

The informer's privilege is also subject to another exception that recognizes the overriding importance of not convicting the innocent. McLachlin J. stated that:

To the extent that rules and privileges stand in the way of an innocent person establishing his or her innocence, they must yield to the *Charter* guarantee of a fair trial. The common law rule of informer privilege, however, does not offend this principle. From its earliest days, the rule has affirmed the priority of the policy of the law "that an innocent man is not to be condemned when his innocence can be proved" by permitting an exception to the privilege where innocence is at stake: *Marks v. Beyfus*, *supra*. It is therefore not surprising that this Court has repeatedly referred to informer privilege as an example of the policy of the law that the innocent should not be convicted, rather than as a deviation from it.¹³⁹

Even when the limited innocence at stake exception applied, however, the court "should only reveal as much information as is essential to allow proof of innocence" and provide the Crown with an opportunity to stop or stay the case before ordering disclosure.¹⁴⁰

The innocence at stake exception to police informer privilege has recently been affirmed and explained by the Supreme Court as follows:

137 Ibid at para 40.

138 *R. v. Parmar* discussed *infra* part 3.

139 Ibid at para 24.

140 Ibid at para 33.

...the only real exception to the informer privilege rule is the innocence at stake exception: *Leipert*. All other purported exceptions to the rule are either applications of the innocence at stake exception or else examples of situations in which the privilege does not actually apply. For example, situations in which the informer is a material witness to a crime fall within the innocence at stake exception: *R. v. Scott*, [1990] 3 S.C.R. 979, at p. 996. The privilege does not apply to an individual whose role extends beyond that of an informer to being an *agent provocateur*: *R. v. Davies* (1982), 1 C.C.C. (3d) 299 (Ont. C.A.); Hubbard, Magotiaux and Duncan, at p. 2-28. Similarly, situations in which s. 8 of the *Charter* is invoked to argue that a search was not undertaken on reasonable grounds may fall within the innocence at stake exception: *Scott*. Thus, as I noted, the only time that the privilege, once found, can be breached, is in the case of an accused raising the innocence at stake exception. All other so-called exceptions are simply applications of this one true exception: *Scott*, at p. 996; D. M. Paciocco and L. Stuesser, *The Law of Evidence* (4th ed. 2005), at p. 254.¹⁴¹

The Court also suggested that a police informer privilege that made no allowance for an innocence at stake exception might violate the *Charter*.¹⁴²

The risk of convicting the innocent and its counter-productivity in terrorism cases was eloquently affirmed in a speech given by Ken Macdonald Q.C., the Director of Public Prosecutions responsible for many terrorism prosecutions in Britain. While in no way discounting the real threat of terrorism or the need for vigorous prosecutions, Mr. Macdonald warned that:

There is a real danger of measures for combating terrorism-related offences being counterproductive. Compromising the integrity of the trial process would blight the criminal justice system for decades. It would severely undermine public confidence. We should recall the impact the Birmingham Six case had on public

¹⁴¹ *Named Person v. Vancouver Sun* 2007 SCC 43 at para 29.

¹⁴² *Ibid* at para 28; *R. v. Leipert* at para 24.

confidence in the 1970s and 1980s. Nothing is more offensive to the Constitution of a country than men and women sitting for years in prison cells for offences they did not commit. What better way could there be to create disillusionment and alienation? We don't want to alienate the very sections of the community whose close cooperation and consent is required to bring successful cases.¹⁴³

Similarly the Supreme Court in *R. v. Stinchcombe*¹⁴⁴ grounded the broad constitutional right of disclosure that it recognized in that case with the accused's right to full answer and defence and a concern for preventing miscarriages of justice when it stated:

The right to make full answer and defence is one of the pillars of criminal justice on which we heavily depend to ensure that the innocent are not convicted. Recent events have demonstrated that the erosion of this right due to non-disclosure was an important factor in the conviction and incarceration of an innocent person. In the *Royal Commission on the Donald Marshall, Jr., Prosecution*, Vol. 1: *Findings and Recommendations* (1989) (the "Marshall Commission Report"), the Commissioners found that prior inconsistent statements were not disclosed to the defence. This was an important contributing factor in the miscarriage of justice which occurred and led the Commission to state that "anything less than complete disclosure by the Crown falls short of decency and fair play" (Vol. 1 at p. 238).

The Court in that case also added that "the principle has been accepted that the search for truth is advanced rather than retarded by disclosure of all relevant material."

It serves neither the interests of society nor the interests of the victims of terrorism to convict the wrong person for an act of terrorism. Experience has shown that wrongful convictions bring the administration of justice into disrepute in many ways. They often make it impossible to apprehend, prosecute and punish the true perpetrators of heinous crimes. Terrorist

¹⁴³ Ken MacDonald Q.C. "Security and Rights" January, 2007 at http://www.cps.gov.uk/news/nationalnews/security_rights.html

¹⁴⁴ [1991] 3 S.C.R. 326

cases, in which the state may have legitimate claims to keep information secret about possible suspects, present a particular risk of producing wrongful convictions.¹⁴⁵

This brief survey indicates the importance of treating those accused of terrorism fairly by allowing them to have access to information that is necessary for them to make full answer and defence. *Stinchcombe* recognizes the fundamental importance of disclosing information to the accused, especially when the information is necessary for the accused to make full answer and defence. Even the informer privilege must yield when innocence is at stake. At the same time, the principle that the accused must be treated fairly will be shaped by the context of the case, including both the nature of the criminal trial and the need to keep secrets.

C) Respect for the Presumption of Open Courts

Another principle that should be considered in resolving the tensions between secrecy in intelligence and fairness with respect to evidence is the presumption of open courts. The open court principle has long been recognized in Canadian law, and was given renewed vigour by the Charter guarantee of freedom of expression. In a case applying the presumption of open courts to investigative hearings under the *Anti-Terrorism Act*, the Supreme Court explained:

Public access to the courts guarantees the integrity of judicial processes by demonstrating “that justice is administered in a non-arbitrary manner, according to the rule of law”: *Canadian Broadcasting Corp. v. New Brunswick (Attorney General)*, *supra*, at para. 22. Openness is necessary to maintain the independence and impartiality of courts. It is integral to public confidence in the justice system and the public understanding of the administration of justice. Moreover, openness is a principal component of the legitimacy of the judicial process and why the parties and the public at large abide by the decisions of courts.

¹⁴⁵ Bruce MacFarlane “Structural Aspects of Terrorist Trials” in Vol 3 of the Research Studies; Kent Roach and Gary Trotter “Miscarriages of Justice in the War Against Terrorism” (2005) 109 Penn. State Law Review 1001.

The open court principle is inextricably linked to the freedom of expression protected by s. 2(b) of the *Charter* and advances the core values therein... The freedom of the press to report on judicial proceedings is a core value. Equally, the right of the public to receive information is also protected by the constitutional guarantee of freedom of expression. The press plays a vital role in being the conduit through which the public receives that information regarding the operation of public institutions... Consequently, the open court principle, to put it mildly, is not to be lightly interfered with.¹⁴⁶

The Court has related the open court principle to freedom of expression under the *Charter* and to public confidence in the administration of justice.

The open court principle is not absolute and limitations on it can be justified. In *Re Vancouver Sun*, the Court applied the existing jurisprudence on publication bans to restrictions on publicity on investigative hearings and held that restrictions on the open court principle could only be justified on the basis that: 1) they were “necessary in order to prevent a serious risk to the proper administration of justice because reasonably alternative measures will not prevent the risk”; and 2) “the salutary effects of the publication ban outweigh the deleterious effects on the rights and interests of the parties and the public, including the effects on the right to free expression, the right of the accused to a fair and public trial, and the efficacy of the administration of justice.”¹⁴⁷ This demanding test requires restrictions on the open court principle to be justified in light of proportionality concerns, including those based on least restrictive measures, and on an overall balance of the harms to the right to free expression against the benefits of the ban.

In *Re Vancouver Sun*, the Court recognized that some proceedings before the courts will by their nature be conducted *in camera*. The Court accepted that the *ex parte* application for an investigative hearing, like other *ex parte* applications such as an application for a search warrant, must be held *in camera*. The Court indicated that “It may very well be that by necessity large parts of judicial investigative hearings will be held in

¹⁴⁶ *Re Vancouver Sun* [2004] 2 S.C.R. 332 at paras 25-27

¹⁴⁷ *Ibid* at para 29.

secret. It may also very well be that the very existence of these hearings will at times have to be kept secret.”¹⁴⁸ On the facts of the case, however, the majority concluded that the application for an investigative hearing and the name of the witness to be compelled should have been secret, but that the existence of the order for an investigative hearing and the conduct of the Charter challenge to the investigative hearing should have been made in public. Even in cases where the very existence of an investigative hearing would have been the subject of a sealing order, the investigative judge should put in place, at the end of the hearing, a mechanism whereby its existence, and as much as possible of its content, should be publicly released.¹⁴⁹

The Supreme Court has warned that “In any constitutional climate, the administration of justice thrives on exposure to light — and withers under a cloud of secrecy.”¹⁵⁰ High standards of justification for infringement on freedom of expression apply in the investigative as well as the trial stage. Justice Fish stated:

In oral argument before this Court, counsel for the Crown referred to this as the “advantage of surprise”. In this regard, Doherty J.A. noted Iacobucci J.’s conclusion in *Mentuck*, at para. 34, that access to court documents cannot be denied solely for the purpose of giving law enforcement officers an investigative *advantage*; rather, the party seeking confidentiality must at the very least allege a *serious and specific risk to the integrity of the criminal investigation*.¹⁵¹

Although the presumption of openness was not absolute, it could not be discharged by the invocation of a generalized assertion that publicity would adversely affect investigations. The Supreme Court has affirmed the open court presumption in the context of a Crown application for a sealing order on materials used to obtain a search warrant. The Criminal Code allows a judge to prohibit access to information relating to warrants and production orders when required for justice, including in cases where disclosure would compromise the identity of confidential informants,

¹⁴⁸ Ibid at para 41

¹⁴⁹ It should be noted that two judges dissented in that case, raising concerns that if “the police cannot investigate and collect information in a confidential environment, their investigation or attempt to prevent the terrorist offence would be undermined because suspects could be “tipped off” and that witnesses could be intimidated. Ibid at para 75.

¹⁵⁰ *Toronto Star Newspapers v. Ontario* [2005] 2 S.C.R. 188 at para 1.

¹⁵¹ Ibid at para 39

harm innocent persons or ongoing investigations, or endanger a person engaged in particular intelligence gathering techniques and thereby prejudice future investigations.¹⁵² This provision, however, must be administered in a manner that is consistent with the Charter. There is no presumption that the material should be closed because the case involves national security,¹⁵³

In *Ruby v. Canada*¹⁵⁴, the Supreme Court held that mandatory publication bans could not be justified even with respect to proceedings that involved national security. Although the protection of information that could harm national security and the supply of information from foreign sources was an important objective and mandatory closed proceedings would “reduce the risk of an inadvertent disclosure of sensitive information”, discretionary publication bans were more respectful of freedom of expression than mandatory ones. This approach has been followed by lower courts in invalidating mandatory publication restrictions under s.38 of the CEA.¹⁵⁵ At the same time, closed courts have been justified with respect to those parts of proceedings which discuss secret information.¹⁵⁶

Restrictions on the open court principle may be easier to justify in cases where restrictions on publicity are necessary to ensure fairness towards the accused. In *Dagenais v. C.B.C.*¹⁵⁷, the Court rejected a hierarchical approach that automatically preferred fair trial rights to freedom of expression. Nevertheless, it recognized the accused’s right to a fair trial as an objective that could in appropriate cases support a publication ban. In that case, a publication ban could not be justified because there were reasonable alternatives to reconcile expression and fairness. In the context of secret national security information, however, it is less obvious that there will be reasonable alternatives to a restriction on the open court process. The principles of keeping secrets and treating the accused fairly will both support restrictions on the open court principle if, for example, they allow the accused or a security-cleared counsel to challenge the state’s case. The overall harm to freedom of expression may be minimal if parts of the proceedings, perhaps subject to some delays, can be made public. At the same time, publication bans may be quite effective in preventing harms to national security or international relations.

¹⁵² Criminal Code s.487.3.

¹⁵³ *O'Neill v. Canada (Attorney General)* (2005) 192 C.C.C.(3d) 255 at para 47 (Ont.Sup.Ct.)

¹⁵⁴ [2002] 4 S.C.R. 3 at paras 54-55.

¹⁵⁵ *Toronto Star v. Canada* 2007 FC 128 at para 2. See also *Ottawa Citizen Group v. Canada (Attorney General of Canada)*, 2004 FC 1052 at paragraphs 35-40.

¹⁵⁶ *Ruby v. Canada* [2002] 4 S.C.R. 3. See also *Khawaja v. Canada* 2007 FC 469

¹⁵⁷ [1994] 3 S.C.R. 200

There is also a procedural dimension to the open court principle. Since its decision in *Dagenais*, the Court has recognized the practical importance of giving the media notice and standing in court proceedings in order to ensure that full consideration is given to the open court principle. Insofar as terrorism prosecutions implicate the open court principle, the judge may be confronted with multiple parties representing multiple interests. These include provincial prosecutors; the Attorney General of Canada, who has special powers and responsibilities under s.38 of the Canada Evidence Act to protect confidences; media representatives and the accused. In addition, to the extent that witnesses have interests, either in terms of protection or in terms of their obligations not to disclose secret evidence, they may also require representation. The multiplicity of the competing interests and competing parties adds to the complexity of managing the relation between secret intelligence and public evidence. As discussed above, however, the media and other third parties do not have standing in proceedings to determine whether the informer privilege exists. Information covered by the informer privilege will remain secret, and is not subject to the balancing and justification process normally required, which justifies restrictions on the open court principle. That said, the Court has recognized a role for media representation and the open court principle in determining that only the minimum of information that is necessary to protect the identity of informer should be kept secret.¹⁵⁸ The Criminal Code empowers judges, in appropriate cases, to exclude the public from the courtroom, if such orders are necessary to prevent injury to international relations, national defence or national security,¹⁵⁹ and to make orders prohibiting the broadcast of information that would identify any witness, victim or justice system participant.¹⁶⁰ Although the Supreme Court held that a publication ban on the identification of a witness should be overturned in the *Air India* investigative hearing case, in large part because the witness did not request such a ban, Justice Josephson issued two permanent publication bans on the identity of witnesses in the *Malik and Bagri* prosecution. In one case he concluded:

The indictment here charges offences of extreme violence, motivated in large measure, the Crown alleges, by a desire for revenge and retaliation. There is evidence of threats and violence being directed towards those who have taken contrary positions to those of certain

¹⁵⁸ *Named Person v. Vancouver Sun* 2007 SCC 43 at para 51.

¹⁵⁹ Criminal Code s.486

¹⁶⁰ *ibid* s.486.5

extremist elements. There is also evidence of what the Witness not unreasonably interpreted to be a serious threat to the lives of herself and her family should she reveal certain information. Only upon receiving an assurance that her identity would remain confidential did she disclose this information to the authorities, maintaining throughout that she would never testify out of fear for the safety of herself and her family.

In this context, the Witness's ongoing security concerns rise beyond the merely speculative. The risk also does not abate simply because she has completed her testimony, as retaliation is a strong element of the risk.¹⁶¹

Although respect for the presumption of open courts should be recognized in terrorism prosecutions, other important interests, including the need to treat the accused fairly, to protect witnesses and informers and to protect the state's interests in national security confidentiality, may justify proportionate restrictions on freedom of expression.

This brief survey has outlined the importance of the presumption of an open court. This principle applies even with respect to national security matters. Although the courts have been resistant to mandatory publication bans with respect to court proceedings where secret information is not discussed, they have generally accepted the importance of restrictions on publicity in cases where the state would be entitled to make *ex parte* representations to judges about the dangers of disclosing secret evidence. If the evidence is disclosed to the accused, courts can still, in appropriate cases, restrict publicity to the wider public. Nevertheless, they may only do so to prevent a serious risk to the proper administration of justice, and only in situations where there are no other reasonable alternatives and when the benefits to the objectives of the publication ban outweigh its harms.

D) The Need for Efficient Court Processes

The final principle that needs to be considered is the need for an efficient process that will allow terrorism prosecutions to reach a final verdict. There is a range of reasonable opinion about the role of the criminal law in counter-terrorism efforts. Some would argue that intelligence rather than

¹⁶¹ *R. v. Malik and Bagri* 2004 BCSC 520 at paras 6 and 7.

the criminal law should be the prime instrument to prevent terrorism; others would argue that administrative regulation targeting sites and substances that can be used for terrorist purposes should be the prime instrument. A few commentators have urged that extra legal measures may be appropriate and necessary to stop terrorism. Regardless of these debates, few would dispute that punishment and incapacitation are the appropriate responses with respect to those who would prepare and plan to commit acts of terrorist violence and those who have committed such violence. Criminal trials also can serve a valuable purpose in denouncing acts of terrorism and educating the public about the dangers of terrorism. They demonstrate a commitment to fairness and principles of individual responsibility in which only the guilty are punished. The criminal trial that only punishes the guilty is the moral antithesis, and the moral superior, of the terrorist who punishes the innocent.

There is also a public interest in having terrorism prosecutions reach a verdict so that damning allegations against people are resolved on the basis of admissible evidence and proper application of the presumption of innocence and the standard of proof of guilt beyond a reasonable doubt. Public trials of terrorists have an important educational function and can, if conducted properly, rebut allegations that terrorists are being persecuted because of their politics or religion. Finally, various international instruments, including conventions in relation to terrorism, also obligate Canada to treat and prosecute terrorism as a serious crime.

One of the reasons why the relation between intelligence and evidence is a central focus in the terms of reference of the Air India inquiry is because the failure to manage this relationship can make it difficult, if not impossible, to use the criminal process as a response to terrorism. As will be seen, the Air India trial that concluded in acquittals in 2005 is something of an exception in the history of Canadian terrorism prosecutions because it went to verdict. It was not delayed and fragmented by national security confidentiality proceedings in the Federal Court of the type seen in the ongoing *Khawaja* prosecution. The trial judge avoided fashioning a remedy for the destruction of intelligence that should have been disclosed to the accused only because the accused were acquitted. The prosecution was not aborted because of a reluctance to disclose the identity of vulnerable informers, as was the case with respect to the *Parmar* and *Khela* cases to be discussed below. Many previous terrorism prosecutions in Canada have been unable to reach a final verdict, in large part because of disputes and unwillingness by the state to disclose secret information, including the identity of informers.

The current Canadian process of resolving claims of national security confidentiality involves litigation in the Federal Court, and this procedure has resulted in a mistrial being declared in one case because of the delay caused when such separate proceedings were launched in the middle of the jury trial.¹⁶² Although a second trial in that case was able to reach verdict, and s.38 of the CEA was reformed in 2001 to encourage pre-trial adjudicative and non-adjudicative resolution of disputes over national security confidentiality, the threat of delays and disruptions of terrorism prosecutions remains. The ongoing Khawaja terrorism prosecution has been delayed by pre-trial proceedings, including the adjudication and appeals of matters under s.38 of the CEA. Khawaja was arrested in March, 2004, and the trial is now not scheduled to start till mid-2008. In contrast, a trial against Khawaja's alleged co-conspirators was completed in April, 2007, despite the fact that it was one of the longest trials in British history, involving 13 months of trial, 105 prosecution witnesses and 27 days of jury deliberation.¹⁶³ Other countries have more experience with terrorism prosecutions than Canada, and we should carefully examine their procedures to determine if they provide a more efficient means of reconciling the competing demands of fairness and disclosure.

Delays in terrorism prosecutions not only frustrate crime control interests, they raise potential due process problems as well. Section 11(b) of the Charter provides the accused with a right to a trial within a reasonable time. The Supreme Court has recognized that there are both social and individual interests at stake in the efficiency of the criminal process. As Justice Sopinka explained:

The individual rights which the section seeks to protect are: (1) the right to security of the person; (2) the right to liberty; and (3) the right to a fair trial.

The right to security of the person is protected in s. 11(b) by seeking to minimize the anxiety, concern and stigma of exposure to criminal proceedings. The right to liberty is protected by seeking to minimize exposure to the restrictions on liberty, which result from pre-trial incarceration and restrictive bail conditions. The right to a fair trial is protected by attempting to ensure that

¹⁶² See *R. v. Ribic* case study discussed *infra* Part 6.

¹⁶³ "Five get life over London bomb plot" April 30, 2007 at http://news.bbc.co.uk/2/hi/uk_news/6195914.stm

proceedings take place while evidence is available and fresh.

The secondary societal interest is most obvious when it parallels that of the accused. Society as a whole has an interest in seeing that the least fortunate of its citizens who are accused of crimes are treated humanely and fairly. In this respect, trials held promptly enjoy the confidence of the public. As observed by Martin J.A: "Trials held within a reasonable time have an intrinsic value. The constitutional guarantee enures to the benefit of society as a whole and, indeed, to the ultimate benefit of the accused ..." In some cases, however, the accused has no interest in an early trial, and society's interest will not parallel that of the accused.

There is, as well, a societal interest that is by its very nature adverse to the interests of the accused. In *Conway*, a majority of this Court recognized that the interests of the accused must be balanced by the interests of society in law enforcement. This theme was picked up in *Askov* in the reasons of Cory J. who referred to "a collective interest in ensuring that those who transgress the law are brought to trial and dealt with according to the law" (pp. 1219-20). As the seriousness of the offence increases, so does the societal demand that the accused be brought to trial. The role of this interest is most evident and its influence most apparent when it is sought to absolve persons accused of serious crimes simply to clean up the docket.¹⁶⁴

It is often in both the accused's and society's interests to resolve criminal cases in an efficient manner. These interests are, if anything, intensified in the context of terrorism prosecutions where the accused may face stigma and/or denial of bail, and where public confidence in the administration of justice may be harmed by allegations that the state has acted improperly or has apprehended the wrong person, perhaps for discriminatory reasons related to their political or religious beliefs. Moreover, s. 11(b) remains a justiciable right. If violated, the minimal remedy is the entry of a stay of proceedings, and this has been used to stop some mega-trials.¹⁶⁵

¹⁶⁴ *R. v. Morin* [1992] 1 S.C.R. 771

¹⁶⁵ *R. v. Chan* (2003) 15 C.R.(6th) 53 (Alta Q.B.); *R. v. Callocchia* (2003) 39 C.R.(5th) 374 (Que.C.A.).

Although the accused can, in certain circumstances, be required to waive s.11 (b) to undertake some proceedings, and judges take a holistic and contextual approach to issues of trial delay, the accused, at the end of the day, has an enforceable right against trial delay. The spectre of a s.11 (b) violation adds constitutional force to the overall principle that terrorism prosecutions should be conducted efficiently for the good of both the accused and the public.

E) Summary

The demands for an efficient, yet fair and public, process for terrorism prosecutions all speak to the ability of Canada to use the criminal law to prosecute terrorism. The challenge is to ensure a process that provides an opportunity for the state to protect legitimate secrets while at the same time treating the accused fairly, respecting as much as possible the principle of open courts and resolving disputes about the reconciliation of these competing principles in an efficient and timely manner. A failure to resolve these difficulties will make it very difficult to bring terrorism prosecutions to verdict. A failure to prosecute terrorists and punish those whose guilt has been established beyond a reasonable doubt in a fair trial will erode public confidence in the administration of justice. It may also place Canada in breach of international obligations that require it to treat acts of terrorist violence as serious criminal offences.

III. The Use of Intelligence as Evidence

At times, intelligence may constitute some of the best evidence in terrorism prosecutions. Although security intelligence agencies target those who present a risk of involvement in terrorism, such targets may unexpectedly commit crimes, including many of the new terrorist crimes created in 2001. There are several barriers to using intelligence as evidence in terrorism prosecutions. One barrier is that security intelligence agencies generally are subject to less demanding standards when they collect information than the police. The rationale for such an approach is that security intelligence is designed to provide governments with secret information to help prevent security threats while the police collect evidence that can be used in public trials. Another barrier to using intelligence as evidence is that security intelligence agencies may have to disclose information surrounding the collection of intelligence as the price of using intelligence as evidence

This section of the study will start with an examination of whether material obtained through a CSIS wiretap could be admitted as evidence in a criminal trial. This raises the question of whether the CSIS wiretap scheme is consistent with the right against unreasonable search and seizure in s.8 of the Charter; whether it can be justified as a reasonable limit under s.1 of the Charter; or whether unconstitutionally obtained CSIS wiretap evidence would be admitted or excluded under s.24(2) of the Charter. The leading case remains the *R. v. Atwal* terrorism prosecution in 1987, and this case will be discussed both as a precedent and a detailed case study.

The use of CSIS wiretaps will be examined in comparison with Criminal Code wiretap warrants. The 2001 ATA has made it easier in several respects to obtain Criminal Code wiretap warrants in terrorism investigations. As in the last section, it is important to revisit conventional wisdom about the relation between evidence and intelligence in light of changed legal and social circumstances as they affect terrorism investigations conducted by both the police and security intelligence agencies. One challenge with both CSIS and Criminal Code wiretaps is that the accused may gain access to confidential affidavits presented by the state to a judge to obtain the warrant. A case study of the Parmar prosecution in Hamilton will reveal how disclosure of material that would have identified a confidential informant caused that terrorism prosecution to collapse. Additional topics to be examined in this section will be the possible role that security cleared special advocates could play in challenges to Criminal Code and CSIS warrants, the collection and retention of intelligence under s.12 of the *CSIS Act*, the use of CSIS material under business records exceptions and the admissibility of various forms of intelligence collected outside Canada as evidence.

A) A Comparison Between CSIS Act and Criminal Code Electronic Surveillance Warrants

Electronic surveillance may, along with the recruitment of human sources, play a critical role in the investigation and prevention of terrorism. Section 21 of the *CSIS Act* allows a judge of the Federal Court to authorize the interception of communications or the obtaining of information on reasonable grounds that a warrant “is required to enable the Service to investigate a threat to the security of Canada” or to perform its duties to collect information about foreign states or persons under section 16 of

the Act.¹⁶⁶ This is a reasonable grounds standard, albeit one related to the investigation of a threat to the security of Canada and not necessarily a crime. It is not a standard based on mere suspicion.¹⁶⁷

Section 186(1)(a) of the Criminal Code simply refers to the requirement that an authorization for electronic surveillance be in the “best interests of the administration of justice”. This phrase has long been interpreted by the Supreme Court as requiring the judge to be satisfied that there are reasonable and probable grounds to believe that an offence has been or is being committed and that the intercept will provide evidence of that offence. In *Duarte*, the Supreme Court held that such a standard:

....meets the high standard of the *Charter* which guarantees the right to be secure against unreasonable search and seizure by subjecting the power of the state to record our private communications to external restraint and requiring it to be justified by application of an objective criterion. The reason this represents an acceptable balance is that the imposition of an external and objective criterion affords a measure of protection to any citizen whose private communications have been intercepted. It becomes possible for the individual to call the state to account if he can establish that a given interception was not authorized in accordance with the requisite standard.¹⁶⁸

CSIS warrants are tied to that agency’s mandate to investigate threats to the security of Canada while Criminal Code warrants are based on reasonable and probable grounds that a crime has been committed and that electronic surveillance will reveal evidence of the crime. Stated in the abstract, the differences between Criminal Code and CSIS warrants are great. As will be seen, however, some post 9/11 developments suggest that some of these differences may be diminishing.

¹⁶⁶ *CSIS Act* s.21(1)

¹⁶⁷ Section 12 of the *CSIS Act* contemplates a lower standard for investigation of “activities that may on reasonable grounds be suspected of constituting threats to the security of Canada”. This section is discussed *infra*.

¹⁶⁸ [1990] 1 S.C.R. 30. See also *R. v. Garofoli* [1990] 2 S.C.R. 1421.

B) The Constitutionality of Warrants Issued Under Section 21 of the CSIS Act

1. Section 8 of the Charter

In 1987, the Federal Court of Appeal considered the constitutionality of s.21 of the *CSIS Act*. The challenge arose in a terrorist prosecution as the accused sought to challenge the admissibility of a CSIS wiretap and the grounds for issuing the warrant. Mahoney J. for the majority of the Court of Appeal rejected the accused's argument that the warrant was invalid on its face because it did not relate the search to a specific offence and evidence of that offence. He concluded:

The warrant in issue was granted in respect of a threat to national security, not the commission of an offence in the conventional sense. To conclude, as *Hunter et al. v. Southam Inc.* anticipated, that a different standard should apply where national security is involved is not necessarily to apply a lower standard but rather one which takes account of reality.

Since the Act does not authorize the issuance of warrants to investigate offences in the ordinary criminal context, nor to obtain evidence of such offences, it is entirely to be expected that s. 21 does not require the issuing judge to be satisfied that an offence has been committed and that evidence thereof will be found in execution of the warrant. What the Act does authorize is the investigation of threats to the security of Canada and, inter alia, the collection of information respecting activities that may, on reasonable grounds, be suspected of constituting such threats. Having regard to the definition of "judge", s. 21(2)(a) of the Act fully satisfies, mutatis mutandis, the prescription of *Hunter et al. v. Southam Inc.* as to the minimum criteria demanded by s. 8 of legislation authorizing a search and seizure.¹⁶⁹

Hugessen J.A. dissented and found a violation of the s.8 of the Charter because s.21 of the *CSIS Act*:

¹⁶⁹ *Atwal v. Canada* (1987) 36 C.C.C.(3d) 161 at 183 (Fed.C.A.).

...does not provide any reasonable standard by which the judge may test the need for the warrant. There is no requirement to show that the intrusion into the citizen's privacy will afford evidence of the alleged threat or will help to confirm its existence or non-existence. Nothing in the language of the statute requires a direct relationship between the information it is hoped to obtain from the intercepted communication and the alleged threat to the security of Canada. On the contrary, the relationship that is required to be established on reasonable grounds appears to be between the interception and the investigation of the threat. In practical terms this means that the statutory language is broad enough to authorize the interception, in the most intrusive possible manner, of the private communications of an intended victim of a terrorist attack without his knowledge or consent. Even more alarming, it would also allow an interception whose purpose was not directly to obtain information about the threat being investigated at all, but rather to advance the investigation by obtaining other information which could then be used as a bargaining tool in the pursuit of the investigation.¹⁷⁰

The majority of the Court of Appeal stressed that *Hunter v. Southam* standards were not appropriate in the national security context. In contrast, the minority concluded that the requirement in s.21 that the Minister have a belief on reasonable grounds that the warrant is required to investigate a threat to the security of Canada was "so broad as to provide no objective standard at all. Even when due account is taken of the importance of the state interest involved, the extent of the possible intrusion on the privacy of the citizen is wholly disproportionate."¹⁷¹

There are few public cases decided under s.21 of the *CSIS Act*. The Canadian Civil Liberties Association challenged s.21 on the basis that it allowed intrusive investigation of activities that were not unlawful, but defined in s.2 of the *Act* as threats to the security of Canada. Potts J. rejected these arguments primarily on the basis of the decision of the majority of the

¹⁷⁰ *ibid* at 198.

¹⁷¹ *ibid* at 199.

Federal Court of Appeal in *Atwal*. He concluded that the investigative powers of CSIS did not in either their purpose or effect violate any of the fundamental freedoms under s.2 of the Charter. Potts J. held there was no violation of s.8 of the Charter because there was no reasonable expectation of privacy with respect to lawful advocacy or protest conducted in public. In addition, s.21 provided for prior judicial authorization of searches on the basis of objective criteria and sworn evidence.¹⁷² The Ontario Court of Appeal in a decision by Charron J.A. dismissed an appeal on the basis that the Canadian Civil Liberties Association did not have public interest standing because directly affected people could, as in *Atwal*, litigate the issue. Abella J.A. dissented with respect to standing, but would have dismissed the CCLA's appeal on the merits because of a failure to establish an evidentiary basis for the violation.¹⁷³ The fact that the issue in *Atwal* has not been re-litigated in the last twenty years, however, suggests that regular attempts have not been made to admit evidence from CSIS wiretaps in criminal trials.

A few cases have been litigated in the Federal Court about the proper administration of s.21 warrants. One such case involved an attempt by CSIS to obtain authorization for a CSIS employee, the Director General of Counter-Terrorism, to substitute a foreign visitor for a previous target of the CSIS warrant. The Federal Court rejected this request as inconsistent with the purposes of s.21 in ensuring that there is judicial authorization of electronic surveillance under the *Act*. McGillis J. stressed the judicial role in authorizing CSIS warrants by concluding that a substitution authorized by the Director General was not authorized in the *CSIS Act* and would, in any event, "offend the minimum constitutional requirement in *Hunter et al v. Southam Inc.*, supra, in that it would empower a Service employee, who, by the very nature of his position acts in an investigative and not in an adjudicative capacity, to assess evidence and to apply the full range of the intrusive powers in the warrant against a person."¹⁷⁴ If there was evidence available to convince a CSIS employee that a visitor presented a threat to the security of Canada "that evidence is equally available to be placed before a judge on an emergency application. Indeed, a judge is on duty, twenty-four hours a day, to hear precisely such matters. The fact that it may be more expedient for a Service employee to perform the function is patently irrelevant."¹⁷⁵ This case underlines the importance of

¹⁷² (1992), 8 O.R. (3d) 289 at paras 101, 116 (Gen.Div.)

¹⁷³ *Canadian Civil Liberties Association. v. Canada* (1998) 126 C.C.C.(3d) 257 at para 109 (Ont.C.A.)

¹⁷⁴ *Re Canada Security Intelligence Act* [1997] F.C.J. no. 1228 at para 10 (F.C.T.D.)

¹⁷⁵ *ibid* at para 11

judicial authorization of a CSIS warrant; a prime factor should the state attempt, in future terrorism prosecutions, to use information obtained from a CSIS warrant in a criminal trial.

Does the CSIS warrant scheme violate s.8 of the Charter? The Federal Court of Appeal split 2:1 on this issue in 1987 and there has not been a definitive adjudication of the issue since that time. Although Charter jurisprudence has evolved considerably since 1987, the basic issues debated in *Atwal* still define the parameters of the debate. The central issue continues to be whether *Hunter v. Southam* crime standards apply to security intelligence intercepts. *Hunter v. Southam* itself, however, contemplated that different standards could apply with respect to national security matters. Although it does not require full *Hunter v. Southam* standards, the CSIS scheme provides some protection for privacy through the requirement of judicial authorization, including the requirement under s.21(2)(b) that less intrusive investigative means will not be successful. In addition, the courts have generally not required crime-based reasonable grounds standards for legitimate regulatory searches. On the other hand, it could be argued that *Hunter v. Southam* crime-based standards should apply if the results of a CSIS wiretap are to be introduced in a criminal trial or when CSIS is focusing its investigations on individuals who may be guilty of terrorism crimes. Even if CSIS wiretaps were obtained in violation of s.8, they could still be defended as a reasonable limit under s.1 of the Charter.

2. Section 1 of the Charter

A section 1 defence of the CSIS warrant scheme would likely focus on the role of security intelligence in providing governments with advance information that could be used to prevent acts of terrorism. Such an objective is pressing and substantial and the CSIS warrant scheme, which requires less than probable cause of a crime, is rationally connected to the objective of prevention. The critical s.1 questions would be whether there was a reasonable alternative that was more respectful of s.8 rights and the overall balance between the harm to a person's rights and the benefits of the CSIS warrant scheme. In this analysis, concerns could be raised that the CSIS warrant scheme is overbroad.

CSIS's terrorism mandate is focused on "activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving

a political, religious or ideological objective within Canada or a foreign state.”¹⁷⁶ The focus in this section is on serious violence towards persons or property. The inclusion of serious violence to property is broader than the definition of terrorist activity in s.83.01 of the Criminal Code which is limited to “substantial property damage” that “is likely to result” in danger or serious bodily harm to a person, serious risk to health or safety or endangerment of human life. It could be argued, however, that the preventive and non law-enforcement mandate of CSIS justifies its broader mandate with respect to property damage.

In addition, a trial judge has found that the reference to terrorist activities being for the purpose of achieving a political, religious, or ideological purpose, objective or cause, in s.83.01 of the Criminal Code, constituted an unjustified violation of the fundamental freedoms.¹⁷⁷ The Special Senate Committee conducting the three-year review of the Anti-Terrorism Act has also recommended that the reference to political, religious or ideological purpose be removed from the *CSIS Act*, and replaced with more neutral language that focuses on actions designed to intimidate a population or compel a government or international organization to act.¹⁷⁸ At the same time, the Commons committee conducting its own three year review made no similar recommendation.¹⁷⁹

Another potential overbreadth challenge to the definition of threats to the security of Canada in the *CSIS Act* is that it includes lawful advocacy, protest or dissent, if carried on in conjunction with activities that constitute threats to the security of Canada. The ATA contains a broader exemption for “advocacy, protest or stoppage of work”, so long as it is not intended to endanger life, public health or safety, or cause death or serious bodily harm. The more limited CSIS exemption could, however, be defended on the basis that it does not criminalize activity, but only defines the investigative and intelligence mandate of a security intelligence agency that does not have police powers.

Evidence obtained under a CSIS wiretap would qualify as a search that was authorized by law and, barring problems with the affidavits or the administration of the warrant, as a search that was conducted in a

¹⁷⁶ *CSIS Act* s.2

¹⁷⁷ *R. v. Khawaja* (2006) 214 C.C.C.(3d) 399 (Ont.Sup.Ct.)

¹⁷⁸ Special Senate Committee on the Anti-Terrorism Act *Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the Anti-Terrorism Act* February, 2007

¹⁷⁹ *Rights, Limits, Security: A Comprehensive Review of the Anti-Terrorism Act and Related Issues* March 2007

reasonable manner. In addition, investigative necessity must be shown to obtain a CSIS warrant whereas it now does not have to be demonstrated to obtain a Criminal Code warrant in a terrorism investigation. Following the majority decision in *Atwal*, courts might find that the law is reasonable given the role of an intelligence agency.

If evidence obtained through a CSIS wiretap was sought to be introduced in a criminal trial, however, it would be important for the state to establish that the CSIS wiretap process was not being used as a shortcut around Criminal Code authorizations. Stanley Cohen has suggested that the courts might rely on a trilogy of cases taken from the field of regulatory inspections and searches. This analysis would suggest that a CSIS search could be reasonable if the predominant purpose of the search was not the determination of penal liability but rather the legitimate “regulatory” goals of CSIS in investigating threats to the security of Canada. The test for determining when “the officials ‘cross the Rubicon’”, and “the inquiry in question engages the adversarial relationship between the taxpayer and the state”, is when “the predominant purpose of the inquiry in question is the determination of penal liability.”¹⁸⁰

The test to determine when criminal law standards should apply is not a bright line one, but depends on the totality of the circumstances. The line will not be crossed simply because there are reasonable grounds or a suspicion that an offence may have occurred. At the same time, the line may be crossed before actual charges are laid. Relevant factors would include whether there were reasonable grounds to lay charges, whether the state’s conduct was consistent with a criminal investigation, the relation between the regulatory officials (in this case CSIS) and criminal investigators and whether the information being collected was relevant to penal liability. Contact between CSIS and the RCMP, while not determinative, would likely count as evidence that the “Rubicon” had been crossed. In addition, the possibility of laying a criminal charge, including new financing, participation and instructing terrorist activities offences, might also count as a factor suggesting that an attempt had been made to circumvent Criminal Code authorization.

CSIS warrants in terrorism cases should be closely monitored to determine when the line into criminal investigations has been crossed. At that

¹⁸⁰ See Stanley Cohen *Privacy, Crime and Terror* (Toronto: Lexus Nexus 2006) at 399-402 *R. v. Jarvis* [2002] 3 S.C.R. 757 at para 88

point, a Criminal Code warrant should be obtained because the Court has stressed that “wherever the predominant purpose of an inquiry or question is the determination of penal liability, criminal investigatory techniques must be used. As a corollary, all Charter protections that are relevant in the criminal context must apply.”¹⁸¹

3. Section 24(2) of the Charter

Even if evidence obtained from a CSIS wiretap were to be found to violate s. 8 of the Charter and not to be justified under s.1 of the Charter, the evidence could still be admissible under s.24(2) of the Charter. Section 24(2) of the Charter provides that unconstitutionally obtained evidence shall be excluded if its admission in all the circumstances would bring the administration of justice into disrepute. The Court has drawn a distinction between the admission of unconstitutionally obtained evidence conscripted from the accused and evidence that was not so conscripted. The admission of conscriptive evidence will generally affect the fairness of the trial and require exclusion, while non-conscriptive evidence will only be excluded after balancing the seriousness of the violation against the adverse effects of excluding the evidence.¹⁸²

In *R. v. Duarte*¹⁸³, the Court admitted wiretap evidence despite finding that it was obtained in violation of s.8 of the Charter. It did not invoke the fair trial test, and instead held that the admission of the evidence would not bring the administration into disrepute because the police acted in good faith reliance on a statute that was presumed to be valid in exempting participant surveillance from the warrant requirements in the Code. In 1995, the Court again admitted evidence obtained from electronic participant surveillance conducted in violation of s.8. The Court concluded that it “seems readily apparent that the admission of the evidence did not affect the fairness of the trial. The appellant could not by any stretch of the imagination be said to have been conscripted into incriminating himself in these conversations”.¹⁸⁴ Other courts have held that the same rationale applies to unconstitutional third party electronic surveillance on the basis that while the accused’s statements were recorded by the state, they were made independently of state intervention.¹⁸⁵

¹⁸¹ *ibid* at para 98

¹⁸² *R. v. Stillman* [1997] 1 S.C.R. 607.

¹⁸³ [1990] 1 S.C.R. 30.

¹⁸⁴ *R. v. Wijesinha* [1995] 3 S.C.R. 422 at para 55.

¹⁸⁵ *R. v. Pope* (1998) 129 C.C.C.(3d) 59 at para 8 (Alta.C.A.).

Even if obtained through an unjustified violation of s.8 of the Charter, evidence obtained under a CSIS warrant will likely be held to be non-conscriptive evidence. Its admissibility would then depend on a balancing of the seriousness of a violation against the adverse effects of admitting evidence. Good faith reliance on statutes and warrants has been held, in many cases, to mitigate the seriousness of the violation.¹⁸⁶ The importance of the evidence to the case and the seriousness of the charges have been held to increase the adverse effects to the administration of justice of excluding even unconstitutionally obtained evidence.

In the *Air India* prosecution, Justice Josephson ruled that even though a search warrant executed against Mr. Reyat violated s.8 of the Charter because it did not specify any time limit on the search, it was nevertheless admissible under s.24(2) because the admission of the evidence would not affect the fairness of the trial, and the violation was not serious. Although he found no s.8 violation in relation to a misdescription in the affidavit of CSIS wiretaps as a confidential and reliable source that could not be revealed for security reasons, it is possible that he would have found that any violation resulting from this approach did not require exclusion under s.24(2) of the Charter in order to avoid condoning a serious Charter violation.¹⁸⁷ This decision affirms the important role that s.24(2) could play in an individual case. That said, s.24(2) would be a finite resource when it comes to the admission of CSIS intelligence in criminal trials, because it will become more difficult over time for the government to argue that it acted in good faith reliance on the CSIS warrant scheme if it has been found to violate the Charter.

4. Use and Disclosure of a CSIS Warrant: A Case Study of *R. v. Atwal*

The following case study demonstrates that CSIS wiretaps could be admitted at a criminal terrorism trial, but also that the consequence of

¹⁸⁶ See for example *R. v. Fliss* [2002] 1 S.C.R. 535 and cases reviewed at Roach *Constitutional Remedies in Canada* (Aurora: Canada Law Book, 2006) at 10.1576-10.1647.

¹⁸⁷ He stated that he “would not have characterized the drafting technique employed in the unique circumstances of this case as a ‘deliberate deception’. That phrase connotes a sense of fraud and dishonesty. I accept that the informant was at the mercy of C.S.I.S. in crafting the information to obtain. C.S.I.S. was a new organization in 1985. The interrelationship between the R.C.M.P. and C.S.I.S. was undefined and the source of some confusion in relation to the *Air India* investigation. While I cannot assess the reasonableness of the insistence by C.S.I.S. that its involvement not be disclosed, the informant was left with little choice but to accept that condition. The alternative was not to use any of the evidence gathered by C.S.I.S., which would have substantially affected the likelihood of obtaining the search warrants sought. Faced with that dilemma, they proceeded in this reasonable fashion. The use of language obscuring the involvement of C.S.I.S. was, like many other elements in this case, unprecedented, unique, and unlikely to re-occur.” *R. v. Malik* 2002 BCSC 1731 at para 71

such admission would be disclosure of the material used to obtain the warrant. As will be seen, the CSIS wiretap evidence in this case was never used in a criminal trial. This was not because of problems with respect to the constitutionality of the CSIS warrant scheme, but rather because of problems with respect to false and misleading information in the affidavit used to obtain the particular warrant.

Four accused Sikh men were charged with attempted murder after the shooting in British Columbia on May 25, 1986, of Mr. Malkiad Singh Sidhu, the Minister of Planning for the state of Punjab in India, upon a visit to British Columbia. These men were apprehended, not because of CSIS information or wiretaps, but rather because they were apprehended by the police shortly after the shooting. The four accused were found guilty by a jury of the attempted murder charge on February 27, 1987. The Crown's case relied on physical evidence connecting the four men with a car that had been abandoned at the scene of the shooting.¹⁸⁸ The four men were each sentenced to 20 years in prison. This sentence was subsequently upheld on appeal to the British Columbia Court of Appeal, in part on the basis of life imprisonment sentences given in 1986 for two men convicted of conspiring to blow up an Air India plane.¹⁸⁹

Charges of conspiracy to commit murder were subsequently laid in September, 1986 against the same four men and five other men including Harjit Singh Atwal after CSIS revealed incriminating wiretaps to the police about a plot to kill Mr. Sidhu. The conspiracy charge was severed from the attempted murder charge against the four men arrested at the scene. This decision was, in part, because of the complexities of different evidentiary standards that might apply to the different offences.¹⁹⁰ It also reveals how choice of charge in some case may affect the need to use intelligence in a criminal trial. The conspiracy charge was based on the CSIS wiretaps, but the attempted murder charge was based on physical evidence.

The remaining conspiracy charge collapsed and was stayed by the Crown after CSIS officials indicated that misleading information had been included in the affidavit used to obtain a warrant under s.21 of the

¹⁸⁸ *R. v. Dhindsa* [1989] B.C.J. no. 2194 denying appeals from conviction. The RCMP's arrest of the four perpetrators was not apparently related to the incriminating information that was discovered through the CSIS wiretap. There were reports at the time that CSIS did not inform the RCMP of the threats against the visiting Indian cabinet minister. Neil Macdonald "Spy Agency kept Indian Minister's visit secret from RCMP" *Ottawa Citizen* Sept. 15, 1987 A1.

¹⁸⁹ *R. v. Atwal* [1990] B.C.J. no. 1526.

¹⁹⁰ *R. v. Atwal* [1987] B.C.J. No. 397. A change of venue was also granted to New Westminster.

CSIS Act.¹⁹¹ The Crown had prepared to use evidence obtained under the broadly worded CSIS warrant. The CSIS warrant applied, not only to Atwal's home, but other places that he might resort to.¹⁹² Atwal had applied to the Federal Court that issued the warrant to rescind the warrant. The issuing judge refused to rescind the warrant. On appeal, the Federal Court of Appeal held 2:1 that s.21 of the *CSIS Act* did not violate s.8 of the Charter. As discussed above, the Court of Appeal rejected various facial challenges to the warrant in part on the basis that inferences could be made that the judge had addressed the necessary criteria under s.21(2) (a) and (b) of the act. It also relied on American authority that held that "domestic security surveillance may involve different policy and practical considerations from the surveillance of 'ordinary crime'. The gathering of security intelligence is often long range, and involves the interrelation of various sources and types of information...the emphasis on domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime."¹⁹³

The Court of Appeal reversed the issuing judge's order that the affidavit used to obtain the CSIS warrant not be disclosed. The trial judge had denied disclosure of the affidavit on the basis that the affidavit:

...relates to political terrorism which was in the course of being investigated in the interests of national security. Disclosure might well result in the revelation of security investigatory methodology which could lead to the significant impairment of the effectiveness of this and future security investigations. The public interest in protecting and preserving the security service's ability to discharge the onerous and important mandate given to it under the C.S.I.S. Act in the interests of national security cannot be disregarded or ignored.¹⁹⁴

Mahoney J. for the Federal Court of Appeal rejected this argument on the basis that "the ends of national security are not tantamount to the ends

¹⁹¹ The disclosure led to Ted Finn, the first director of CSIS, resigning. When two of the men charged were released from prison they were greeted by Talwinder Singh Parmar. Kim Bolan "Separatist slogans welcome free Sikhs" *Vancouver Sun* Sept 16, 1987 E8.

¹⁹² Terry Glavin "Eavesdropping legality upheld" *Vancouver Sun* May 1 1987 A11.

¹⁹³ *R. v. Atwal* (1987) 36 C.C.C.(3d) 161 at 178 quoting *U.S. v. U.S. District Court* 407 U.S. 292 at 322 (1972).

¹⁹⁴ *ibid* at 189

of justice".¹⁹⁵ He reasoned that the accused's entitlement to challenge the affidavit should not be different from those that would apply to the accused at trial. Although intelligence obtained through CSIS warrants might in some cases be used as evidence, full disclosure of the intelligence, as well as the basis for obtaining the intelligence, may be the price that is paid for admissibility of intelligence as evidence.

The disclosure ordered by the Federal Court of Appeal was not absolute. It indicated that "the only statutory limitation on disclosure is an absolute prohibition against disclosure by any person of information from which the identity of an informer or an employee engaged in covert operations can be inferred. That prohibition should be respected by the court."¹⁹⁶ The Court of Appeal ordered that the judge who issued the warrant should disclose the affidavit to Atwal "after deleting therefrom anything from which the identity of any person described in s. 18(1)(a) and/or (b) of the Act can be inferred"¹⁹⁷. In addition, this disclosure was made subject to the ability of the Attorney General to claim public interest immunity under the *Canada Evidence Act*. Such claims were not made. In any event, the wiretap evidence was never tendered by the Crown at any trial. The warrant was rescinded when the Attorney General of Canada revealed that false information had been used to obtain the warrant. The provincial Attorney General declined to proceed with the case. Although it could be argued that even unwarranted intercepts could be admitted as evidence under s.24(2), it would have been difficult to argue that the Charter violation was not serious or was committed in good faith in light of the concessions that the affidavit used to obtain the CSIS warrant was inaccurate.

The *Atwal* case study demonstrates that evidence obtained under a CSIS wiretap could in some cases be used in criminal trials. It is, however, possible that the accused might have been able to object to the warrant, including its broad resort to clause, before the trial judge, had the wiretap evidence been tendered at trial. The argument would have been that even if the CSIS warrant was reasonable on its face, that the breadth and the manner of the search would have been unreasonable. The extensive litigation in the Federal Court over the warrant would not have necessarily settled the question of the admissibility of the warrant at trial. That said,

¹⁹⁵ *ibid* at 190

¹⁹⁶ *ibid* at 186. This was a reference to the restrictions on disclosure under s.18(1) of the *CSIS Act*. This restriction is, however, subject to the authorized grounds of disclosure under s.19 including disclosures to police and Attorneys General with respect to investigations and prosecutions.

¹⁹⁷ *Ibid* at 192

a trial judge would have the option of admitting evidence from a CSIS wiretap under s.24(2), even if the evidence was obtained in violation of s.8 of the Charter and the violation was not justified under s.1.

The attempt to use the CSIS wiretap as evidence allowed the accused both to challenge the CSIS warrant scheme and the breadth of the particular warrant under the Charter. The fact that the CSIS scheme will attract Charter challenge may make it advisable, if possible, to use Criminal Code wiretap warrants that have been repeatedly upheld under the Charter. That said, the structure of the Charter allows the state several opportunities to justify the use of CSIS wiretaps in criminal trials. As discussed above, even if s.21 of the *CSIS Act* violates s.8 of the Charter, the government can argue that it is a reasonable limit on the right. Even if this argument fails, the government can argue that the wiretap evidence is admissible under s.24(2) of the Charter as non-conscriptive evidence that was obtained in good faith reliance on a valid statute and a valid warrant. The good faith argument was not available in *Atwal*, but more because of particular circumstances of the case that are not likely to be repeated.

The *Atwal* case study demonstrates that disclosure may be the price paid for the evidentiary use of intelligence. The Federal Court of Appeal unanimously concluded that the affidavit in support of the CSIS warrant should be disclosed to the accused to allow the accused to challenge the legality and constitutionality of the warrant. As will be seen in the subsequent discussion of the *Parmar* case study, disclosure of such information mirrors standards of disclosure used with respect to Criminal Code wiretap warrants. The initial engagements of CSIS with the criminal justice system and its disclosure obligations were not happy experiences for CSIS. They may have influenced CSIS attitudes towards engagement with the criminal justice system. That said, CSIS, like its peer agencies such as MI5, must be prepared for the fact that intelligence gathered in its terrorism investigations may in some cases be used as evidence.

Although disclosure is necessary to respect the accused's right to full answer and defence and to challenge the legality and constitutionality of the search, it is not an absolute value. The Court of Appeal indicated that the confidential affidavit containing intelligence that was used to obtain the warrant could be edited to respect s.18 of the *CSIS Act* so as not to reveal the identity of confidential sources of information or any CSIS employee engaged in covert operational activities. A corollary

of such editing, however, would be that information edited out of the affidavit and not disclosed to the accused could not be used to support the warrant. Depending on how the affidavit was constructed, editing out material could result in a conclusion that the warrant was not legally or constitutionally granted. As will be seen, this is what happened in the *Parmar* case. That said, the affidavits used in *Atwal* and *Parmar* were drafted at a time when the accused had not gained access to the sealed packet of confidential material used to obtain wiretap warrants. Today, the affidavits would be drafted with the possibility of editing to protect public interests in non-disclosure in mind. In any event, even if the CSIS warrant in *Atwal* could not be upheld as consistent with s.8 of the Charter once information that could identify confidential informants or covert agents was edited out, the state could still argue that the unconstitutionally obtained evidence could be admitted under s.24(2).

Although the Federal Court of Appeal unanimously ordered that the affidavit used to obtain the warrant should be disclosed to the accused, it was not blind to the dangers of disclosing intelligence. As discussed above, it contemplated that the affidavit would be edited to protect confidential informants and covert agents. It also noted that the Attorney General of Canada could apply under what is now ss.37 or 38 of the *Canada Evidence Act* to obtain a non-disclosure order on the basis of harms to national security and other public interests. Such orders would also mean that the warrant could not be supported by confidential information that was the subject of a non-disclosure order, and the admissibility of the evidence might have to be determined under s.24(2). As will be examined below, the process of applying for a non-disclosure order under s.38 of the CEA would require separate litigation in the Federal Court.

The *Atwal* case study demonstrates that the evidentiary use of intelligence may come with the price of disclosure to the accused. Disclosure is not, however, absolute. Affidavits containing intelligence can be edited before disclosure to the accused and non-disclosure orders can be sought through separate litigation under the CEA. Material that is edited out of the affidavit and not disclosed to the accused cannot be used to support the warrant. At the same time, the state can argue, in the absence of other improprieties such as the inaccuracies in the affidavit in *Atwal*, that electronic surveillance, even that obtained under an unconstitutional wiretap, could still be used as evidence under s.24(2) of the Charter.

5. Summary on the Admission of CSIS Wiretaps

Although it is 20 years old, the Federal Court of Appeal's decision in *Atwal* is still the leading precedent holding the CSIS warrant scheme to be constitutional. Such a conclusion would require courts to accept the distinct purpose of intelligence gathering as opposed to law enforcement either when interpreting s.8 of the Charter or under s.1 of the Charter. Courts may be more inclined to find a Charter violation if they are persuaded that CSIS "crossed the Rubicon" by focusing on the penal liability of specific individuals. Even then, however, evidence obtained through a CSIS warrant might still be admitted under s.24(2) on the basis that the admission of unconstitutionally obtained evidence obtained in good faith reliance on legislation and a warrant would not bring the administration of justice into disrepute.

The Federal Court of Appeal's decision in *Atwal* also affirms that the disclosure of the affidavit used to obtain the CSIS warrant will be required to allow the accused to challenge the warrant as part of the right to make full answer and defence. Disclosure is not absolute, because the affidavit can be edited to protect confidential sources and covert agents, and because the Attorney General of Canada can make national security confidentiality claims.

C) The Case for Earlier Use of Criminal Code Electronic Surveillance Warrants

Any assessment of the constitutionality of the CSIS wiretap warrant scheme cannot be undertaken in the abstract. In deciding whether a particular CSIS wiretap violates the Charter, courts are likely to ask whether grounds existed for obtaining a Criminal Code wiretap warrant. When intelligence is being collected, security intelligence agencies must ask themselves whether they have "crossed the Rubicon" into a predominant focus on criminal liability. Although this test is a flexible one that depends on all the circumstances and will not be triggered simply by discussions with the police, or even by the existence of reasonable grounds to believe that a crime has been committed, it is a question that should be asked at regular intervals during counter-terrorism investigations. If at all possible, the state should not rely on complex after-the-fact adjudications on whether a line has been crossed, or about the possibility that security intelligence may be found to be admissible in a criminal trial under s.24(2) of the Charter. In cases of uncertainty, but where there are sufficient

grounds for a Criminal Code authorization, preference should be given to the collection of evidence under Criminal Code warrants. Such a process will, however, require close co-operation between CSIS and the police. Information obtained by the police from Criminal Code warrants that has intelligence value can always be passed on to the security intelligence agencies, whereas the passing of information obtained by CSIS to the police has been more problematic in the past.¹⁹⁸

The 2001 *Anti-Terrorism Act* amendments have made Criminal Code electronic surveillance warrants more attractive from the state's perspective. Criminal Code warrants in terrorism investigations can now, like CSIS wiretap warrants, be issued for up to a year.¹⁹⁹ Unlike CSIS warrants²⁰⁰, there is no longer a requirement of establishing that other investigative procedures such as surveillance, informers, undercover agents and regular search warrants would not be successful in order to obtain a Criminal Code warrant in relation to a terrorism investigation.²⁰¹ Finally, the grounds for warrants obtained under *Hunter v. Southam* crime-based standards have expanded with the enactment of many new terrorist crimes that apply long before an actual act of terrorism has occurred. Although it has always had a preventive dimension, as represented by the law of conspiracy and attempts, the ATA has created many new crimes relating to support, financing, participation and preparation for acts of terrorism.²⁰²

The domains of intelligence and evidence collection are shifting both because of the availability of new crimes and legislative changes that make it easier to obtain Criminal Code authorizations for electronic surveillance in terrorism prosecutions. The result may be that some investigations in which a warrant under s.21 of the *CSIS Act* would have been used can now from the start be conducted under a Criminal Code authorization.

The use of Criminal Code warrants is not a panacea. The next case study underlines how disclosure issues led to the collapse of a terrorism prosecution of a person who is widely believed to have been the mastermind of the bombing of Air India Flight 182. Although Criminal

¹⁹⁸ See the discussion of RCMP and CSIS co-operation in Part 1 of this study.

¹⁹⁹ Criminal Code s.186.1.

²⁰⁰ *CSIS Act* s.21(5). CSIS warrants in relation to subversion under s.2(d) of the Act are limited to sixty days.

²⁰¹ Criminal Code s.186 (1.1). Notification of the target can be delayed up to 3 years under s.196(5) of the Code, though no notification is required for CSIS wiretaps.

²⁰² See infra part 1 for a more detailed discussion of new terrorism crimes.

Code warrants will require the state to establish reasonable grounds to believe that a crime has been, or will be, committed and reasonable grounds that the collection will reveal evidence of the crime, it has become easier to obtain Criminal Code electronic surveillance warrants in terrorism investigations than at the time of the Parmar and Atwal cases discussed in this section. As will be seen, the Parmar case might be decided differently today as a result of Parliament's abolition of an automatic statutory exclusionary rule that applied to unwarranted or unlawful electronic surveillance. Today the state would have a stronger argument that the wiretap evidence should be admitted under s.24(2) of the Charter, even if the need to protect the identity of an informer meant that the edited affidavit could no longer support the warrant. There are also provisions in the Criminal Code that now allow the prosecutor to edit the affidavit used to obtain the warrant in order to protect a wide range of public interests. The accused can only seek more disclosure if the judge determines that a summary would not be sufficient and the material is required for the accused to make full answer and defence.²⁰³

The jurisprudence and procedures used to challenge Criminal Code warrants and to edit confidential material before it is disclosed to the accused are better established and more certain than the scant jurisprudence surrounding the use of CSIS material in criminal trials. In addition, the legislation providing for Criminal Code wiretaps has been upheld by the Supreme Court,²⁰⁴ whereas the Federal Court of Appeal in *Atwal* only affirmed the CSIS wiretap provision in a divided decision made over twenty years ago. Where possible, Criminal Code electronic surveillance warrants should be used in counter-terrorism investigations. Intelligence agencies need to constantly explore the relation between their intelligence gathering and comparable collection of evidence by the police.

D) Parmar - A Case Study of Disclosure and Criminal Code Warrants

On June 14, 1986, seven Sikh men were charged in Hamilton with conspiring to commit various violent crimes in India. The alleged plans involved bombing Indian Parliament buildings, derailing trains in India, blowing up an oil refinery in India, as well as kidnapping a child of a member of the Indian Parliament in order to force him to assist them in the above plans. Two accused were discharged, but the remaining men,

²⁰³ Criminal Code ss.187(4) and 187(7).

²⁰⁴ *R. v. Garofoli* [1990] 2 S.C.R. 1421; *R. v. Thompson* [1990] 2 S.C.R. 1111

including Talwinder Singh Parmar, were ordered to stand trial on three counts of conspiracy on December 22, 1986.

On March 10, 1987, Justice Watt dealt with an application by the accused for an order to open the sealed packets of material (containing two affidavits), which formed the basis for an authorization to intercept private communications. The basis for this application was that it was necessary for the applicants to make full answer and defence to the charges they faced at trial. Watt J. characterized the accused's argument for access to the sealed packet in the following terms:

It is said that a critical aspect of the right to make full answer and defence, an incident of the constitutional right of fundamental justice guaranteed by s. 7 of the Charter, is the right to challenge the receivability of that portion of the prosecution's proof which is the primary evidence said to have been obtained by interceptions made in accordance with those authorizations and/or renewals the informational basis of which is sought to be disclosed. It would seem that the argument ultimately to be made against the receivability of the primary evidence rests upon a submission that the interception process constituted an unreasonable search or seizure, thereby an infringement of s. 8, and ought to be excluded in accordance with s. 24(2) of the Charter.²⁰⁵

Conversely, the Crown argued that opening a sealed packet should be sparingly exercised in light of the statutory provisions for confidentiality. The Crown argued that the accused should demonstrate on the balance of probabilities that access to the sealed packet was required to make full answer and defence.

Justice Watt acknowledged that s.178.14 of the Criminal Code then in force only allowed for breaching the confidentiality of the sealed packet when (a) dealing with an application for renewal of the authorization, and (b) pursuant to an order of a judge. Before the Charter, it was only in exceptional circumstances, such as allegations of fraud or material non-disclosure, that a judge would order that a sealed packet supporting the warrant be opened. Nevertheless, he held that the accused should have access to the sealed packet in order to make a meaningful challenge that

²⁰⁵ *R. v. Parmar* (1986) 34 C.C.C.(3d) 260 at 273 (Ont.H.C.)

the warrant violated s.8 of the Charter. Justice Watt found that such an approach did “no violence to the plain wording” of the Code and that it was “further, compatible with the fundamental justice guarantee of the s. 7 of the Charter.”²⁰⁶ He also found that ordering disclosure accords with the strong public policy in favour of openness in respect of judicial acts, even when those acts were initially performed on an *ex parte* and *in camera* basis.²⁰⁷

Justice Watt concluded that the accused should have access to the sealed packet that authorized the wiretap warrant on the basis that if the accused were required to demonstrate “fraud or material non-disclosure before an order may issue permitting the opening of the sealed packet, the accused are in a catch-22 situation. In most cases evidence of material non-disclosure in particular will not emerge by magic. It is only upon that access to the sealed packet that the accused will be able to develop a meaningful capacity to advance a defence on this issue.”²⁰⁸ Access to the sealed packet was supported by the accused’s right to full answer under s.7 of the Charter, the right against unreasonable search and seizure under s.8 of the Charter, as well as the need for public accountability for a warrant process even though the warrant was initially on an *in camera* and *ex parte* basis.

Justice Watt acknowledged that the accused were being granted access to the sealed packet in the absence of any evidence of wrongdoing in the obtaining of the warrant and that:

²⁰⁶ *ibid* at 276

²⁰⁷ He explained: “It may also be observed that to order disclosure under the relevant subparagraph in the present circumstances, subject to editing, also accords with the strong public policy in favour of openness in respect of judicial acts, even those which have been initially performed on an *ex parte* and *in camera* basis. Whilst it is no doubt true, as has been held in the case of conventional search warrants, that the effective administration of justice would be frustrated in the event that individuals were allowed to be present upon the issuance of investigative warrants in respect of themselves, the force of such argument substantially abates upon the execution of the order. Thereafter, there exists but a diminished or attenuated interest in confidentiality. It is a fortiori when the evidentiary fruits produced by the issuance of such investigative warrant are to be adduced in a public trial. Further, it has been authoritatively held that the strong public policy in favour of openness in respect of judicial acts, such as the issuance of conventional search warrants, contemplates maximum accountability and accessibility. At every stage there ought to be public accessibility and concomitant judicial accountability. The former should only be curtailed in the event of a present need to protect social values of superordinate importance and, in my respectful view, then only to the minimal extent necessary to achieve such purpose:” *ibid* at 278

²⁰⁸ *ibid* at 273 quoting *R. v. Wood et al.* (1986), 26 C.C.C. (3d) 77 at 87-88.

It may seem somewhat anomalous or incongruous that the mere assertion of a right to fundamental justice, without a scintilla of evidence to support an argument of its denial, should serve as a sufficient basis upon which to breach the statutory secrecy of the sealed packet. Indeed, it may appear to be all the more so when compared to that which is required in the event that fraud or material non-disclosure is asserted as the basis upon which the packet should be opened. It must be recalled, however, that what is being here contested is the right to access to the packet in order to raise a potential challenge upon constitutional grounds that certain evidence ought not to be received. In practical terms, it may, to some extent, be a fishing expedition. It is, however, a fishing expedition in what are now constitutionally-protected waters. The ultimate questions of whether the order should be set aside and whether evidence said to be gathered in accordance therewith ought to be received, are quite other matters. To permit access in the present circumstances is but to construe s.178.14(1)(a)(ii) in a manner compatible with the constitutional guarantee of fundamental justice enshrined in s. 7.²⁰⁹

Disclosure was required by the Charter. Even if disclosure could be characterized as “a fishing expedition”, it was one conducted in “what are now constitutionally protected waters.” Although his decision to grant the accused access to the sealed packet was innovative at the time, it was subsequently followed by the Supreme Court.²¹⁰

The accused’s Charter based right to access to the sealed packet was not absolute. As in *Atwal*, some allowance would be made for public interests in non-disclosure. Justice Watt stated it was his duty to review the affidavit, and make any editing changes he felt were necessary in the best interests of the administration of justice. He indicated that he would edit the material before it was disclosed to the accused taking account factors such as:

(a) whether the identities of confidential police informants, and consequently their lives and safety, may

²⁰⁹ *ibid* at 279-280

²¹⁰ *Dersch v. Canada* [1990] 2 S.C.R. 1505

be compromised, bearing in mind that such disclosure may occur as much by reference to the nature of the information supplied by the confidential source as by the publication of his or her name;

(b) whether the nature and extent of ongoing law enforcement investigations would thereby be compromised;

(c) whether disclosure would reveal particular intelligence-gathering techniques thereby endangering those engaged therein and prejudicing future investigation of similar offences and the public interest in law enforcement and crime detection, and

(d) whether disclosure would prejudice the interests of innocent persons.

Editing, in my respectful view, ought to take place to the minimal extent necessary to give effect to societal values of superordinate importance thereby ensuring that by its nature and extent it does not, in practical terms, work an equivalent injustice to that which would ensue from an absolute prohibition against disclosure.²¹¹

After initial editing, the judge would show the edited affidavit to Crown counsel, and if the Crown agreed, he would give a copy to the counsel for the applicants. If further editing was requested, such a determination would be made in open court with the applicants and their counsel present. Defence counsel would not receive a copy until the final editing was done.

The editing procedure used by Justice Watt was subsequently approved of by the Supreme Court in *R. v. Garofoli*²¹² and *R. v. Durette*.²¹³ It was also the basis for amendments to the Criminal Code,²¹⁴ which contemplated the opening, and also the editing, of sealed packets. Section 187(4) of the Criminal Code now provides that the information in the sealed packet should not be disclosed to the accused “until the prosecutor has as deleted any part of the copy of the document that the prosecutor believes would be prejudicial to the public interest including any part that the prosecutor believes could:

²¹¹ *R. v. Parmar* (1986) 34 C.C.C.(3d) 260 at 281-282 (Ont.H.C.).

²¹² [1990] 2 S.C.R. 1421.

²¹³ [1994] 1 S.C.R. 469.

²¹⁴ S.C. 1993 c.40 s.7.

- a) compromise the identity of any confidential informant;
- b) compromise the nature and extent of ongoing investigations;
- c) endanger persons engaged in particular intelligence-gathering techniques and thereby prejudice future investigations in which similar techniques would be used; or
- d) prejudice the interests of any innocent person.

The accused can apply to the trial judge for access to material that is edited out but it will only be disclosed under s.187(7) if “required in order for the accused to make full answer and defence” and if “the provision of a judicial summary would not be sufficient”. This provision may provide for more extensive editing to protect intelligence than was contemplated by the Federal Court in *Atwal*.

The accused challenged the admissibility of the wiretap evidence at a voir dire conducted at the start of the scheduled trial. During the voir dire, the accused established entitlement to cross-examine the affiant on the affidavit that supported the wiretap on the basis that there was “deliberate falsehood or reckless disregard for the truth” in the affidavit. Justice Watt’s decision, which was upheld on appeal to the Ontario Court of Appeal, reveals how warrant practices can be subject to a high level of scrutiny when the fruits of the warrant are sought to be introduced as evidence in a criminal trial.²¹⁵

The errors in the affidavit to support the Parmar warrant were significant. The affidavit alleged that Parmar was connected to the Duncan blast, but “the affiant failed to disclose that on March 24, 1986, three days prior to the affidavit being sworn, Crown counsel had tendered no evidence against the applicant Talwinder Singh Parmar in respect of such a charge.”²¹⁶ The second error in the affidavit supporting the warrant was that it failed to disclose that extradition proceedings against Parmar for alleged crimes in India were unsuccessful.²¹⁷ As in the *Atwal* case discussed above, the disclosure process is a rigorous one which will test the accuracy of the affidavits used to obtain the warrant process.

The wiretap was declared unlawful before the start of the trial largely as a result of a Court of Appeal decision that made clear that reliance could not

²¹⁵ *R. v. Parmar* (1987) 37 C.C.C.(3d) 300 at 319 aff’d (1990) 53 C.C.C.(3d) 489 (Ont.C.A.)

²¹⁶ *ibid* at 346

²¹⁷ *ibid* at 346

be placed on material that had been edited out by the judge to sustain the wiretap.²¹⁸ As with the initial decision to disclose the affidavit, this decision was innovative, but has subsequently become the norm. Justice Watt recognized that this process would apply an “artificial informational basis, the edited affidavit, rather than the material actually before the authorizing judge”, but he concluded that it was the only possible procedure that would ensure fairness to both the accused’s right to full answer and defence and the Crown’s right to protect informers.²¹⁹

Justice Watt concluded “that Crown counsel ought to be afforded the opportunity to persist in non-disclosure yet take the position that the authorization had been properly issued on the basis of the information contained in the affidavit as edited.” On the facts of the case, however, the Crown conceded that it could not defend the warrant without the information that was edited to protect the informer. The Crown’s decision may in part reflect the fact that the affidavit was drafted at a time when it was expected that it would never be disclosed to the accused or edited. In the result, Watt J. held that Crown counsel had failed to establish that lawful authority existed for the intercept because “the prosecution could not support the issuance of the order without reference to the edited material. The prosecutor’s case, accordingly, failed and the accused were found not guilty.”²²⁰

Before the prosecution was ended, however, two alternative methods of reconciling the demands of full answer and defence and public interest immunity, including informer privilege, were considered. The first was that the Crown sought, but was denied, consent from the informer to make necessary disclosures that would reveal his identity. A media story at the time reported that the investigators “could not persuade the informant to make his identity public, Crown Attorney Dean Paquette told the court. The informant rejected an offer to be moved to another community in Canada

²¹⁸ *R. v. Hunter* (1987) 34 C.C.C.(3d) 14 (Ont.C.A.)

²¹⁹ He elaborated: “It cannot be gainsaid that, to some extent at least, non-disclosure of the type here considered deprives defending counsel of information whereby to test the propriety of the issuance of the authorization, hence reasonableness and constitutionality of the investigative techniques of the state. On the other hand, the imposition of a proportionate or equivalent disability upon the state, namely, denial of reliance upon the non-disclosed information as a basis to support the issuance of the interceptional mandate, ensures that neither advantage is gained by the state nor lost by the accused in the process. The parties are, so nearly as is practically possible, left in a position of equality and as if the non-disclosed material had not been furnished to the authorizing judge. Absent an *in camera ex parte* hearing to examine the impact of the additional non-disclosed material, the present scheme ensures procedural and substantive fairness.” *R. v. Parmar* (1987) 31 C.R.R. 256 at 284 (Ont.H.C.)

²²⁰ *ibid* at 284.

under a witness relocation program. Even presenting the defence with a summary of the informant's knowledge would jeopardize the individual's identity... 'No one knows what potential harm could befall the informant should their identity become publicly known,' Paquette told the court '... If I were placed in a similar situation, I would not be prepared to consent to the information identifying me.'²²¹ The resolution of the Parmar case underlines how issues of disclosure and national security confidentiality are closely connected to the adequacy and attractiveness of witness and source protection.

A second alternative was to draw an adverse inference from the editing process that the wiretap evidence was obtained illegally and without a warrant, but to argue that it should be admissible in any event. This option had recently been recognized by the Ontario Court of Appeal as a possible response to the editing of an affidavit²²² in a regular search warrant case. Justice Watt, however, concluded that "the alternative of a warrantless search in the interception of private communications is of no practical utility in light of the provisions of paragraph 178.16(1) (a) of the Criminal Code." This section of the Criminal Code provided that intercepted private communication were "inadmissible as evidence against the originator of the communication or by the person intended by the originator to receive it unless the interception was lawfully made..." This automatic exclusionary rule has since been repealed.

Today, it would be possible to conclude that the warrant was not valid, but that the wiretap could be admitted under s.24(2) of the Charter without bringing the administration of justice into disrepute. The court would balance the seriousness of the violation of s.8 in intercepting private communications without a valid warrant against the adverse effects on the administration of justice of excluding such evidence. The Crown's case under s.24(2) would be quite strong because the wiretap evidence would constitute non-conscriptive evidence that would not affect the fairness of the trial. Moreover, the evidence was obtained in apparent good faith reliance on a warrant issued under a valid statute. The errors in the affidavit, however, as in *Atwal*, would provide a basis to argue that admitting the product of the warrant would condone a serious violation of the Charter. Under the serious violation test, however, the Crown could stress the adverse effects to the administration of justice of excluding important and perhaps crucial evidence in a case where most serious

²²¹ Brian McAndrews "Five acquitted in terror trial" *Toronto Star* April 15, 1987 p.A1.

²²² *R. v. Hunter* (1987) 34 C.C.C.(3d) 14 (Ont.C.A.)

crimes were alleged to have been committed. In any event, the option of arguing that the wiretap evidence should be admitted under s.24(2) was, however, precluded in the *Parmar* case because of the automatic exclusionary rule under then section 178.16(1)(a) of the Criminal Code.

Today, *Parmar* might be decided differently. The Crown would argue that even if the warrant could not be supported on the basis of the edited affidavit, evidence obtained under it should be admitted under s.24(2) of the Charter without bringing the administration of justice into disrepute. Today, the underlying affidavit for the wiretap might be drafted differently because the authorities would be aware both that the affidavit may be disclosed and that reliance could not be placed on portions of the affidavit that were edited out to protect informants or other public interests in non-disclosure. Section 187(4) provides broad grounds for editing the affidavit before it is disclosed to the accused and subsequent disclosure will only be ordered under section 187(7) if judicial summaries are not sufficient and the information is required in order for the accused to make full answer and defence.²²³ Material that is edited out, however, cannot be used to support the validity of the warrant. When it became apparent that the warrant could not be sustained without revealing the informant's identity, the informant in *Parmar* apparently vetoed the disclosure of his or her identity. *Parmar* demonstrates how disclosure is closely linked to the adequacy, or perceived adequacy, and the attractiveness of witness and source protection programs.

E. Disclosure and the Use of Special Advocates in Challenging Criminal Code and CSIS Warrants

The *Parmar* and *Atwal* case studies reveal how wiretaps can obtain important evidence in terrorism investigations, but that attempts to use such information as evidence will require considerable disclosure to the accused and a high degree of scrutiny of state conduct in obtaining the evidence. Whether warrants are issued under the *CSIS Act* or the *Criminal Code*, the state may be faced with the prospect of revealing the identity of key informants and of having those who swear affidavits in support of a warrant cross-examined on the accuracy and truthfulness of the material that supports the warrant. Both case studies reveal how disclosure standards challenged terrorism prosecutions long before the 1991

²²³ There may, however, be a case for expanding s.187(4)(c) to allow the protection of all secret intelligence gathering techniques even when disclosure might not endanger the person engaged in the technique.

decision in *Stinchcombe*. The demands of disclosure were not, however, absolute and in both cases, the affidavits would have been edited to protect confidential sources and ongoing operations before being disclosed to the accused. At the same time, information edited out from the affidavit could not be used to support the wiretap authorization.

There may be other ways to reconcile the interests of the accused in challenging the legality and constitutionality of CSIS or Criminal Code warrants and protecting the confidentiality of information used to obtain the warrant including information from informants, information received in confidence from other agencies and information relating to ongoing investigations. The law at present allows the affidavit to be edited to protect state interests in non-disclosure, but then holds that the state cannot rely on material that is edited out of the affidavit to support the warrant because the accused will not have an opportunity to see and challenge the information. The Supreme Court in the warrant context has stressed the importance of the accused's ability to challenge the warrant as part of the accused's right to full answer and defence.²²⁴ At the same time, the Supreme Court in other contexts has recognized that there may be alternatives to disclosure to the accused that still allow effective adversarial challenge of the state's case and that comply with s.7 of the Charter or constitute a reasonable limit under s.1 of the Charter.²²⁵

One of these alternatives may be the use of special advocates who because they are security cleared and permanently bound to secrecy could have access to the entire affidavit used to obtain a CSIS or a Criminal Code warrant without editing. The special advocate could then stand in for the accused and provide adversarial challenge to the warrant by arguing that the warrant was illegally and unconstitutionally obtained and the evidence should be excluded. If necessary, the special advocate could have access to the disclosure provided to the accused and demand further disclosure and cross-examine officials on the basis of the affidavit. The Supreme Court has recognized that while a challenge to a warrant is part of the accused's right to fair answer and defence, it is nevertheless a review that is distinct from a trial on the merits. As Charron J. has explained:

At trial, the guilt or innocence of the accused is at stake. The Crown bears the burden of proving its case

²²⁴ *R. v. Garofoli* [1990] 2 S.C.R. 14121; *R. v. Durette* [1994] 1 S.C.R. 469; *R. v. Pires* [2005] 3 S.C.R. 343.

²²⁵ *Charkaoui v. Canada* [2007] 1 S.C.R. 350

beyond a reasonable doubt. In that context, the right to cross-examine witnesses called by the Crown “without significant and unwarranted constraint” becomes an important component of the right to make full answer and defence... If, through cross-examination, the defence can raise a reasonable doubt in respect of any of the essential elements of the offence, the accused is entitled to an acquittal.... However, the *Garofoli* review hearing [to challenge the warrant] is not intended to test the merits of any of the Crown’s allegations in respect of the offence. The truth of the allegations asserted in the affidavit as they relate to the essential elements of the offence remain to be proved by the Crown on the trial proper. Rather, the review is simply an evidentiary hearing to determine the *admissibility* of relevant evidence about the offence obtained pursuant to a presumptively valid court order....the statutory preconditions for wiretap authorizations will vary depending on the language of the provision that governs their issuance. The reviewing judge on a *Garofoli* hearing only inquires into whether there was any basis upon which the authorizing judge could be satisfied that the relevant statutory preconditions existed... Even if it is established that information contained within the affidavit is inaccurate, or that a material fact was not disclosed, this will not necessarily detract from the existence of the statutory pre-conditions....In the end analysis, the admissibility of the wiretap evidence will not be impacted under s. 8 if there remains a sufficient basis for issuance of the authorization.²²⁶

The limited nature of the challenge to wiretap warrants opens up the possibility that the use of a special advocate to challenge the warrant could be an adequate substitute for allowing the accused to challenge the warrant on the basis of the affidavit as edited to protect the state’s interests in secrecy. Such an approach will not and should not guarantee that the fruits of CSIS and Criminal Code wiretaps will always be admissible. The special advocate may be able to demonstrate that the warrant was illegally or unconstitutionally obtained or administered and that exclusion of the

²²⁶ *R. v. Pires; R. v. Lising* [2005] 3 S.C.R. 343 at paras 29-30.

evidence is necessary to avoid condoning a serious Charter violation that will bring the administration into disrepute. Both the warrants in *Atwal* and *Parmar* had serious flaws. Nevertheless, the use of a special advocate will allow the warrant to be both defended and challenged on the basis of the full record, including material that would today be edited out to protect the state's interests in avoiding disclosure of information about confidential informants and ongoing investigations.

F) The Collection and Retention of Intelligence under Section 12 of the CSIS Act

Apart from the issues of electronic surveillance discussed above, there are questions about whether the methods CSIS uses to collect and retain intelligence affect the possible use of intelligence as evidence. Section 12 of the *CSIS Act* provides:

The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report and advise the Government of Canada.

As will be seen, this section raises distinct issues about the collection and the retention of intelligence.

Section 12 could be challenged under the Charter either on its own or when information and intelligence that CSIS originally collected is sought to be introduced as evidence in a criminal trial. A threshold issue would be whether CSIS's investigation or actions invaded a reasonable expectation of privacy. The courts might hold that open source material, at least as it is related to material that is not related to a biographical core of information, does not infringe a reasonable expectation of privacy.²²⁷

If *CSIS* actions affected a reasonable expectation of privacy, any resulting activity would constitute a search under s.8 of the Charter. Such searches would have to be authorized by law; by a law that was reasonable, and

²²⁷ *R. v. Plant* [1993] 3 S.C.R. 281; *R v. Tessling* [2004] 4 S.C.R. 432

be conducted in a reasonable manner.²²⁸ Section 12 would constitute legal authorization as long as there were, as required under the statute, reasonable grounds to suspect that the activities constituted threats to the security of Canada and the collection of the information was “strictly necessary”.

Section 12 of the *CSIS Act* only requires reasonable suspicion of threats to the security of Canada as opposed to reasonable grounds in relation to crime and evidence of crime. Moreover, it does not require judicial authorization of the investigation. As such, intelligence collected under this provision could be found to violate s.8 of the Charter if the courts applied a *Hunter v. Southam* criminal law standard. On the other hand, the courts might find that information collected under this section to be a legitimate exercise of regulatory powers to collect intelligence. This argument would be the strongest in contexts in which authorities had not, as discussed above, “crossed the Rubicon” and assumed the predominant purpose of determining criminal liability.

The requirement in s.12 that CSIS only collect information “to the extent that is strictly necessary” would also help strengthen the argument that s.12 does not violate s.8 of the Charter. As with the use of evidence obtained under s.21 warrants, the use of s.12 evidence would come with the price of disclosure. The accused would be allowed to challenge the legality and constitutionality of the manner in which CSIS obtained the information. The defence would likely also have access to information that was relevant to the reliability of the information.

To the extent that the intelligence was based on hearsay, the courts would determine in a case-by-case manner which material was sufficiently reliable and necessary to justify its introduction in the criminal trial.²²⁹ The determination of the reliability of the evidence would likely require consideration of the conditions under which the intelligence was obtained. Evidence obtained as a result of torture would be inadmissible even if the torture was committed by other parties, but the status of evidence derived from torture is less clear.²³⁰ The fact that intelligence was confirmed by other facts might support admissibility.²³¹ The consideration of the necessity of introducing the intelligence in a criminal trial could also require consideration of why the evidence was collected by CSIS and not police investigators. Information obtained by CSIS in a regulatory

²²⁸ *R. v. Collins* [1987] 1 S.C.R. 265.

²²⁹ *R. v. Starr* [2000] 2 S.C.R. 144.

²³⁰ *A. v. Secretary of State* 2005 UKHL 71; Criminal Code s.269.1(4).

²³¹ *R. v. Khelawan* [2006] 2 S.C.R. 787.

manner that did not focus on the criminality of individual people might be easier to admit than investigations that focused on the determination of penal liability.

The restrictive statutory standard that the collection of the information is “strictly necessary” limits the collection of information. Once that information is collected, however, CSIS has separate obligations to subject the information to analysis and to retain the information. These separate requirements of analysis and retention appear not to be subject to the “strictly necessary” qualification. Indeed, analysis beyond what is “strictly necessary” is to be preferred. At the same time, information should not be retained if its collection was not “strictly necessary” or was otherwise unlawful. As will be seen in the next part of this study, there can also be a duty under s.7 of the Charter to retain information, including intelligence, which should be disclosed to the accused.

It could be argued that the destruction of intelligence such as CSIS wiretaps or notes taken by CSIS agents is supported by the requirement in s.12 of the *CSIS Act* that information should only be collected “to the extent that is strictly necessary”. Contrary to such arguments, the words “strictly necessary” qualify the reference to investigation in s.12 of the *CSIS Act* and not the reference to the analysis and retention of information and intelligence. From a functional perspective, the primary invasion of privacy is the collection of the information in the first place. That said, care should be taken to ensure that only information that satisfies the standard of being “strictly necessary” is retained. There were legitimate concerns, especially at the time that CSIS was created, that it not retain information that had not been collected under the rigorous standard of strict necessity. Even with respect to new information obtained from confidential and foreign sources, it may be difficult in practice to separate collection and retention issues. For reasons of practical necessity, it may be necessary to destroy some material shortly after it was collected because it should not have been collected in the first place because its collection was not strictly necessary. After this initial period, however, properly collected information should be analysed and retained without reference to the strictly necessary standard.

Despite the above interpretation, it is undeniable that s.12 has caused a number of difficulties. This critical section is not drafted as clearly as it could have been with respect to the grammatical placement of the “strictly necessary” qualifier. Moreover the purposes that are to be served

by the phrase “strictly necessary” in protecting privacy and its relation to the statutory mandate of CSIS are not clear. Section 12 could be amended so that the requirement of strict necessity applies only to the collection of intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada. Once collected information is determined to satisfy the statutory requirement that its collection was “strictly necessary”, it should then be retained and subject to analysis as required to allow CSIS to conduct its lawful duties. These lawful duties include the possible disclosure of CSIS information under s.19(2) (a) of the CSIS Act for criminal investigations and prosecutions. Such an amendment would clarify CSIS’s obligations with respect to the retention of properly collected intelligence.

Another possibility is to make specific reference to the enhanced need to retain information in CSIS’s counter-terrorism investigations. Although criminal prosecutions could arise out of CSIS investigations into espionage, sabotage or subversion²³², they are more likely to occur with respect to its terrorism investigations. It may become necessary for a CSIS counter-terrorism investigation quickly to be turned over to the police so that people can be arrested and prosecuted before they commit acts that could kill hundreds or thousands of people. Section 12 could be amended to specify that CSIS should retain information that may be relevant to the investigation or prosecution of a terrorism offence as defined in s.2 of the Criminal Code or a terrorist activity as defined in s.83.01 of the Criminal Code. A reference to terrorism offences would be broader than a reference to terrorist activities because it would include indictable offences committed for the benefit of, or at the direction of, or in association with a terrorist group even if the offence itself would not constitute a terrorist activity. Information that is retained by CSIS because of its relevance in terrorism investigations or prosecutions could be of use to either the state or the accused in subsequent criminal prosecutions.²³³

Such an amendment would make clear that CSIS’s mandate includes the retention of information and possible evidence that is relevant to terrorism investigations and prosecutions provided that the information was properly collected because its collection was strictly necessary for CSIS to investigate activities that may on reasonable grounds be suspected of

²³² This is implicitly recognized in the *Security Offences Act* R.S. 1985 c.S-7 which gives the RCMP and the Attorney General of Canada priority with respect to the investigation and prosecution of offences that also constitute a threat to the security of Canada as defined in the CSIS Act.

²³³ Hon Bob Rae *Lessons To Be Learned* (2005) at 15-17.

constituting threats to the security of Canada. This would be consistent with amendments to Britain's *Security Service Act* which have made it clear that one of the functions of MI5 is to assist law enforcement agencies in the prevention and detection of serious crime and that information collected by MI5 in the proper discharge of its duties can be "disclosed for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceeding".²³⁴ A similar provision about disclosure of information for criminal proceedings is also contained in the mandate of Britain's foreign intelligence agency.²³⁵ The emphasis in the British legislation is on disclosure of information properly obtained by intelligence agencies whereas in Canada, there seems to be a need to emphasize that CSIS should both retain and disclose information that could assist in preventing or prosecuting serious crimes.

Increased retention of information by CSIS presents some dangers to privacy. An important protection for privacy would be that the requirement to retain information would only apply to information that satisfied either at the time of its collection or immediately afterwards, the "strictly necessary" requirement in the present s.12 of the CSIS Act. The *Privacy Act*²³⁶ would also provide additional protections, albeit subject to the ability to disclose information under its consistent use and law enforcement provisions.²³⁷ In addition, CSIS's review agency, SIRC, as well as its Inspector General, could play an important role in ensuring that information retained by CSIS was retained for purposes related to its statutory mandate and that this information was not improperly distributed. Finally, the Office of the Privacy Commissioner may also audit and review even the exempt banks of data held by CSIS.²³⁸ Retained information should generally be kept secret. If information that is retained by CSIS is shared with others, it should be screened for relevance, reliability and accuracy. Proper caveats to restrict its subsequent disclosure should be attached.²³⁹ Retained information by CSIS could in appropriate cases be passed on to the police under s.19(2)(a) of the CSIS Act or could be

²³⁴ *Security Services Act*, 1989 s.2(2)

²³⁵ *Intelligence Services Act*, 1994 s.2(2).

²³⁶ R.S.C. 1985 c. P-21

²³⁷ *Ibid* s.8. For a discussion of these restrictions see Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar *Analysis and Recommendations* (2006) at 337-338.

²³⁸ Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar *A New Review Mechanism for the RCMP's National Security Activities* (2006) at pp. 286, 433-436. For a discussion of other restraints on information sharing by CSIS see Stanley Cohen *Privacy, Crime and Terror* (Toronto: Lexis Nexus, 2005) at 408.

²³⁹ See generally Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar *Analysis and Recommendations* (2006) at 334-343 in the context of information sharing by the RCMP.

subject to a court order of disclosure as was the case in *R. v. Malik and Bagri*.

G) Admission of CSIS Information under Business Records Exceptions

Intelligence can often be based on hearsay in the sense that it will report what another person purportedly heard another person say. Courts have in recent years become more willing to admit hearsay in cases where the hearsay is necessary and reliable. One of many exceptions that can allow the admission of hearsay evidence is the business records exceptions. In some cases, CSIS information could be admitted as evidence pursuant to s.30 of the *Canada Evidence Act*. That section contemplates the admissibility of records made “in the usual and ordinary course of business” with business defined to include “any activity or operation carried on or performed in Canada or elsewhere by any government...”. This provision has been interpreted to allow evidence that would otherwise be hearsay. One restriction in s.30(10) of the Act provides that nothing in the section renders admissible “a record made in the course of an investigation or inquiry”. This exception has been held to cover notes and logs of police investigations²⁴⁰, as well as computer printouts from military equipment used to assist law enforcement officials in surveillance. It can be argued that investigations are important matters and that those conducting the investigation should have to testify and be subject to cross-examination. In the latter case, however, the records were admitted under the common law exception for business records made contemporaneously by a person under a duty to do so and with personal knowledge of the matters.²⁴¹

Even if the restrictions in s.30(10) of the CEA were repealed and statutory or common law business records exceptions were used to introduce CSIS materials, CSIS officials could still likely be required to explain the significance of the material and the way it was obtained in order to explain why the material was reliable and why it was necessary to admit the material in a trial under the business records exception. This could require CSIS agents to testify to introduce the evidence. Steps could be taken to shield the identity of the CSIS employees from the public, but the accused would require sufficient information about the witnesses in order to be able to engage in meaningful cross-examination and challenges to credibility.

²⁴⁰ *R. v. Palma* (2000) 149 C.C.C.(3d) 169 (Ont.S.C.J.)

²⁴¹ *R. v. Sunila* (1986) 26 C.C.C.(3d) 331 (N.S.S.C.) applying *Ares v. Venner* [1970] S.C.R. 608.

H) Intelligence Collected Outside of Canada

The nature of international terrorism, including the terrorism behind the bombing of Air India Flight 182, suggests that a person identified by Canadian officials as a terrorist suspect may move between Canada and other countries. When a suspect moves away from Canada, Canadian officials may ask foreign officials to engage in surveillance of that person. Such international co-operation may be valuable, but there are dangers that a Canadian suspect may not necessarily be a high priority for a foreign agency or that a foreign agency might in some circumstances use methods that would be objectionable to Canadians and Canadian courts. There appears to be a gap in Canada's intelligence gathering capacities with respect to individual suspects who leave Canada. It appears not to be possible to obtain a warrant under the CSIS act in such circumstances. In turn, the activities of Canada's signals intelligence agency, the Communications Security Establishment (CSE) are restricted and may not be admissible because they are only subject to Ministerial as opposed to judicial authorization.

1) CSIS Wiretaps Directed at Activities Outside Canada

A recently released decision has concluded that the CSIS wiretap warrant scheme in s.21 of the *CSIS Act* cannot be used to obtain warrants to engage in electronic surveillance of Canadian targets outside of Canada. Blanchard J. of the Federal Court Trial Division found that s.21 of the *CSIS Act* did not clearly authorize the granting of warrants for CSIS to conduct electronic surveillance outside Canada. The case involved ten people who were subject to warrants under s.21 of the *CSIS Act*, but who apparently left Canada for an unnamed foreign country. All but one of the suspects were Canadian citizens, permanent residents or refugees.

Blanchard J. found that neither s.12 or s.21 of the *CSIS Act* specifically addressed the issue of whether CSIS powers would apply outside of Canada and, as such, failed to establish a clear legislative intent to violate principles of international law, such as "sovereign equality, non-intervention and territoriality", which would be violated should Canadian officials conduct electronic surveillance in a foreign country.²⁴² The result of this decision is that CSIS appears unable to obtain a warrant to conduct electronic surveillance abroad.

²⁴² Dans l'affaire d'une demande de mandats Oct. 22, 2007. SCRS 10-07 at para 54.

The judgment also suggests that such extra-territorial activities will not violate s.8 of the Charter or any provision of the Criminal Code, nor necessarily CSIS's mandate to collect security intelligence relating to threats to the security of Canada.²⁴³ If the decision is interpreted, however, to preclude the use of CSIS intercepts abroad, this may make Canada reliant on the conduct of such activities by foreign agencies or by Canada's signals intelligence agency, the CSE. As will be seen, the CSE regime has restrictions designed to protect the privacy of Canadians and it operates through a Ministerial authorization scheme that may make it more difficult to introduce the intelligence so obtained as evidence compared to the judicial authorization scheme of s.21 of the *CSIS Act*.

2) Intelligence Collected by CSE pursuant to Ministerial Authorization

Section 273.65(1) of the *National Defence Act*, which was amended as part of the 2001 *Anti-Terrorism Act*, provides that the Minister of Defence "may, for the sole purpose of obtaining foreign intelligence, authorize the Communications Security Establishment in writing to intercept private communications in relation to an activity or class of activities specified in the authorization." Section 273.65(2) provides:

- 2) The Minister may only issue an authorization under subsection (1) if satisfied that
 - (a) the interception will be directed at foreign entities located outside Canada; _
 - (b) the information to be obtained could not reasonably be obtained by other means;
 - (c) the expected foreign intelligence value of the information that would be derived from the interception justifies it; and
 - (d) satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.

²⁴³ Ibid at paras 62-63.

The above provision could authorize the invasion of privacy of Canadians who are at one end of a foreign conversation that is targeted by the Ministerial authorization. As with the constitutionality of s.21 of the *CSIS Act*, much will depend on whether the courts accept an exception from *Hunter v. Southam* standards for national security matters. Section 273.65 of the *NDA* is more vulnerable to Charter challenge than s.21 of the *CSIS Act* because there is no judicial authorization. At the same time, however, s.273.65 does have a variety of restraints, including the requirements of investigative necessity, foreign intelligence value and requirements for conditions to protect the privacy of Canadians. In addition, Canada's main allies in the collection of signals intelligence generally rely on Ministerial as opposed to judicial authorizations.²⁴⁴ Finally, it is possible that the courts could read in any requirements to protect privacy that it found wanting under the section.²⁴⁵

The Special Senate Committee reviewing the Anti-Terrorism Act was told that no more than 20 Ministerial authorizations had been issued under the Act and that as of April, 2005 only five were active. The Arar Commission reported that as of March, 2006 only four ministerial authorizations were active under the foreign intelligence mandate of the CSE.²⁴⁶ Given the small number of these authorizations and depending on their precise ambit, it is possible that a court might find, on the facts of a particular case, that investigators had indeed "crossed the Rubicon" and were focused on collecting information to determine the criminal liability of an individual.

The Special Senate Committee that reviewed the *Anti-Terrorism Act* rejected arguments for judicial authorization on the basis that warrants under present Canadian law do not have extra-territorial effect. Such laws could, however, be amended to provide for such authorization. Judicial authorization for extra-territorial surveillance of a suspect whether conducted by the CSE or CSIS would maximize the chances that courts would accept such intercepts as evidence.

The Special Senate Committee recommended that CSE have specific and public "information retention and disposal policies" in order to protect

244 Stanley Cohen *Privacy, Crime and Terror* supra at 231.

245 Ibid at 236

246 Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar *A New Review Mechanism for the RCMP's National Security Activities* at 144.

the privacy of Canadians.²⁴⁷ Section 275.65(2)(d) already contains a restrictive standard that private communications only be retained if they “are essential to international affairs, defence or security.” Although well intentioned, information disposal programmes should also accommodate the possibility that information obtained by the CSE could subsequently become relevant to a criminal investigation of an act of terrorism. Although any attempt to admit information obtained by the CSE pursuant to Ministerial authorization would be subject to vigorous Charter challenge by the accused, one of the lessons of the erasures of many of the CSIS wiretaps in the Air India case is the need to retain intelligence that may become relevant to criminal investigations either in Canada or abroad. The intelligence can become relevant because of its possible value to the prosecution or because of its possible value to the accused. It would be better for intelligence to be retained, and for the issues of the ultimate admissibility of that evidence to be decided at a subsequent trial, than for the intelligence to be destroyed. Although the retention of intelligence can have negative effects on privacy, steps can be taken to minimize the danger to privacy by, for example, ensuring that access to the intelligence is limited. CSE, like CSIS, is also subject to self-initiated review, which should be able to detect any improper sharing of information.

The above observations relate to one of the main themes of this study, namely the need for the practices of intelligence agencies to catch up to the current emphasis on terrorism as a prime threat to national security and to new crimes of terrorism. One of the relevant features of the new crimes of terrorism in the *Anti-Terrorism Act* is the fact that Canada has asserted jurisdiction to prosecute crimes of terrorism committed outside of Canada. Given the threat and nature of international terrorism, this approach may make eminent sense, but at the same time it may require rethinking of the CSE Ministerial authorization regime. One option would be to allow for CSE to obtain judicial authorization. Another option would be to amend the *CSIS Act* to make clear that CSIS, perhaps with the CSE’s assistance²⁴⁸, can conduct electronic surveillance abroad subject to Canadian judicial authorization and the consent of the foreign country. Both approaches would increase the likelihood that intelligence collected abroad could be admitted as evidence in a Canadian court.

²⁴⁷ Special Senate Committee *Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the Anti-Terrorism Act* Feb. 2007 at 78-79, Recommendation 19.

²⁴⁸ Section 273.64 authorizes the CSE to assist police and intelligence agencies but subject to limitations imposed on those agencies, In *Dans l'affaire d'une demande de mandats* Oct. 22, 2007. SCRS 10-07 at para 70, Blanchard J. indicated in obiter that he found the arguments by CSIS, that it could be assisted by the CSE in conducting electronic surveillance abroad, to be persuasive.

A judicial warrant to authorize either CSIS or CSE to conduct electronic surveillance outside of Canada would not ensure that the intelligence would be admitted in a subsequent trial. The accused would be free to argue that the evidence was obtained in violation of the Charter and should be excluded under s.24(2) of the Charter. Nevertheless, a judicial warrant might be a valuable first step to the ultimate admissibility of intelligence in a criminal trial. The use of warrants could allow the state to argue that, even if intelligence obtained outside of Canada was obtained in violation of s.8 of the Charter, its admission in a terrorism trial would not bring the administration of justice into disrepute under s.24(2) of the Charter.

3) The Admissibility of Foreign Signals Intelligence

The Arar Commission reported that CSE may at times request information from its foreign intelligence partners at the requests of the RCMP and that “if the intelligence generated from these sources relates to the RCMP mandate, the CSE may share it with the RCMP.”²⁴⁹ Information obtained by foreign agencies, even acting in co-operation with Canadian officials, would not in themselves be subject to Charter standards.²⁵⁰ At the same time, an accused in a Canadian trial could argue that the admissibility of such evidence would constitute an abuse of process or violate Charter rights.

Canadian courts might admit foreign intercepts if officials from a foreign agency were prepared to testify as to the manner in which the information was obtained. The actions of the foreign officials would not be subject to the Charter. There might, however, be Charter violations and admissibility problems if there was some evidence that Canadian officials had perpetrated some abuse, such as deliberate circumvention of Canadian laws by reliance on foreign officials. Courts might be more likely to make such findings in circumstances in which Canadian officials had “crossed the Rubicon” and focused on the criminal activities of specific individuals. Courts would also be concerned if it was established that request to foreign partners had been made to avoid Canadian laws restricting the use of electronic surveillance in Canada. In such cases, a warrantless foreign intercept might be effectively substituted for what should have been a Criminal Code authorization for electronic surveillance. On the

²⁴⁹ Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar *A New Review Mechanism for the RCMP's National Security Activities* at 145.

²⁵⁰ *R. v. Harter*, [1995] 3 S.C.R. 562; *R. v. Terry*, [1996] 2 S.C.R. 207.

other hand, evidence obtained from foreign signals intelligence that was not tasked and targeted in such a manner might well be admissible in Canadian criminal trials because the evidence itself would be reliable and the foreign agency that obtained it would not be subject to the Charter. As a result of a recent Supreme Court decision, the same might be said about intelligence collected by Canadian officials acting outside Canada because the Charter appears no longer to apply to such activities.²⁵¹

1) Summary

In complex international terrorism investigations there may be overlapping electronic surveillance by CSIS, the CSE, foreign intelligence agencies and the police as targets frequently move between Canada and foreign states. The Arar Commission has recently recognized that suspects may be transferred to and from CSIS and the RCMP depending on whether there is sufficient evidence to justify a criminal investigation or a security intelligence investigation. The Atwal case study, as well as the facts of the Bagri and Malik prosecution, suggests, that in some cases electronic surveillance obtained under a CSIS warrant may be sought to be admitted into a criminal trial. Although it is 20 years old, the Federal Court of Appeal's decision in *Atwal* is still the leading precedent holding the CSIS warrant scheme to be constitutional. Such a conclusion would require courts to accept the distinct purpose of intelligence gathering, as opposed to law enforcement, either when interpreting s.8 of the Charter or in considering whether a departure from *Hunter v. Southam* standards can be justified under s.1 of the Charter. Courts may be more inclined to find a Charter violation if they are persuaded that CSIS "crossed the Rubicon" by focusing on the penal liability of specific individuals. Even then, however, evidence obtained through a CSIS warrant might still be admitted under s.24(2) of the Charter.

Care should be taken in relying on the admissibility of CSIS intercepts in criminal trials, especially in terrorism investigations where there is a focus on specific individuals and there may be reasonable grounds to believe that a crime, including the many new crimes of preparation and support for terrorism, has been committed. One of the main themes of this study is that security intelligence agencies need to be aware of the possibility of prosecutions arising from their anti-terrorism work and the disclosure and evidentiary implications of such prosecutions. In all cases in which

²⁵¹ *R. v. Hape* 2007 SCC 26.

CSIS obtains an electronic surveillance warrant in a counter-terrorism investigation, it should carefully consider whether there would be grounds for a Part VI Criminal Code warrant and whether the latter would be preferable. Such a process will require close co-operation between CSIS and the relevant police forces.

Given the enactment of many new terrorism offences, the elimination of the investigative necessity requirement and the extended one year time period available for Criminal Code wiretap warrants in terrorism investigations, it is not clear that Criminal Code warrants will always be much more difficult to obtain than CSIS warrants. Any extra effort spent in obtaining a Criminal Code warrant may pay off should there be a prosecution in which material obtained under the warrant is sought to be introduced. Use of the Criminal Code warrant will avoid litigation over whether the CSIS warrant scheme complies with the Charter. The Criminal Code regime also provides for editing of the material used to obtain the warrant before it is disclosed to the accused. One of the most important means of establishing a reliable and workable relation between intelligence and evidence in the counter-terrorism field is to constantly re-evaluate whether a prosecution may occur. Security intelligence agencies need to be aware of the possibility of a terrorism prosecution and the ensuing evidentiary and disclosure implications. The *Parmar* case also suggests that considerations about the protection of sources and witnesses cannot be ignored even during early stages of a terrorism investigation. It is possible that the *Parmar* case might have proceeded to trial had the informant consented to the disclosure to the accused of identifying information in the affidavit or if adequate means had been devised to allow full adversarial challenge to the warrant without disclosing information to the accused that would have identified the informant and potentially put that person's life at risk.

Suspects in international terrorism investigations may frequently move between Canada and foreign countries. A recent judicial decision has held that CSIS cannot obtain a warrant under s.21 of the *CSIS Act* to conduct electronic surveillance outside of Canada. Unless the *CSIS Act* is amended to clearly authorize extra-territorial surveillance, Canada may have to rely on surveillance conducted by foreign agencies and /or the use of CSE signals intelligence. There are problems with both options. Foreign agencies may not have the same priorities as Canadian agencies and they may employ methods that would not be used by Canadian agencies. The CSE relies upon Ministerial as opposed to judicial authorizations

and this may make it more difficult to have CSE intercepts admitted as evidence in court. CSE may also be even more reluctant than CSIS to go to court. Thought should be given to making it possible for Canadian security intelligence agencies to conduct electronic surveillance outside Canada, subject to judicial authorization and the consent of the foreign country where the surveillance will take place. This would keep in place the structure that governs the CSE, including the restrictions designed to ensure that the CSE only collects foreign intelligence and respects the privacy of Canadians.

The different mandates of security intelligence agencies and the police, as well as the different constitutional standards used to obtain information, have often been cited as a reason why intelligence cannot be used as evidence. In this section, we have seen that the CSIS warrant scheme has been upheld under the Charter and that intercepts obtained by CSIS, if retained, could possibly be introduced as evidence in terrorism prosecutions. Even if courts find that CSIS intercepts were obtained in violation of s.8, there would be a strong case, at least in the absence of deliberate circumvention of Criminal Code standards, inaccuracies in affidavits used to obtain the warrant, or reliance on clearly unconstitutional laws or warrants, that they should be admitted under s.24(2). The evidentiary use of intelligence comes with the price of disclosure to the accused and judicial requirements that information that is shielded from disclosure to the accused cannot be used to support the legality or constitutionality of the warrant. There is, however, a possibility that courts might accept that the use of a security-cleared special advocate with full access to all relevant information would be an adequate substitute for disclosure to the accused for the limited purpose of challenging the admissibility of evidence obtained under a warrant.

IV. Obligations to Disclose Intelligence

Even if the state does not attempt to use intelligence as evidence, the accused in terrorism prosecutions may request production and disclosure of intelligence. The broad definition of terrorism offences may make it difficult for the Crown to argue that intelligence about the accused or his or her associates is clearly not relevant and not subject to disclosure. Intelligence may also relate to the credibility of informants and other witnesses and to the methods that were used to investigate the accused.

As discussed in the first part of this study, the Crown's obligation to disclose relevant information to the accused has played an important role in relations between CSIS and the RCMP. SIRC studies in 1998 and 1999 identified the Supreme Court's landmark 1991 *Stinchcombe* case, which constitutionalized the law of disclosure, as a major impediment to the CSIS and RCMP relationship. *Stinchcombe* created fears that any information that CSIS shared with the RCMP might be disclosed to the accused. The important role of *Stinchcombe* was affirmed again in the Malik and Bagri trial.²⁵² At the same time, it is a mistake to locate the disclosure obligations that are inherent in a fair criminal process entirely in *Stinchcombe*. Both the *Atwal* and *Parmar* case studies discussed above pre-date *Stinchcombe*. They demonstrate that the criminal process can in some circumstances require the disclosure of secret information in order to ensure the fair treatment of the accused; one of the four animating principles that underlie this study. They also demonstrate that steps such as editing can be taken to reconcile the demands of disclosure with public interests that will be harmed by disclosure.

As will be seen, the somewhat unique circumstances of the Air India investigation led to findings that CSIS material was subject to *Stinchcombe* disclosure obligations. CSIS's destruction of intelligence, in the form of CSIS wiretaps and notes taken by CSIS agents who interviewed witnesses, was also held to violate obligations under *Stinchcombe* to retain information that should be disclosed. Even if, in other cases, intelligence is not subject to the disclosure and retention requirements of *Stinchcombe*, the accused could attempt to obtain the production and eventual disclosure of intelligence under the common law procedure in *O'Connor* that applies to third parties who may have material of relevance to a criminal trial.

A) Disclosure of Intelligence under *R. v. Stinchcombe*

Stinchcombe involved whether the Crown had an obligation to disclose notes of a police interview of a person who had been called as a Crown witness at a preliminary inquiry but who the Crown planned not to call at trial. Although the case did not involve terrorism or national security matters, it involved the question of whether the Crown had obligations to disclose information in its possession that it did not plan to use at the criminal trial. As such, *Stinchcombe* is very relevant to whether secret intelligence possessed by the Crown must be disclosed to the accused in a terrorism trial even if the Crown makes no attempt to use the secret

²⁵² See part I of this study.

intelligence as evidence at trial. As the *Atwal* case study suggests, however, the Crown could still seek to obtain a judicial non-disclosure order for intelligence that would be subject to disclosure under *Stinchcombe*. As will be seen in part 6 of this study, however, such applications can delay and fragment terrorism trials.

Although *Stinchcombe* is often cited for the broad proposition that all relevant information in the Crown's possession must be disclosed to the accused, the decision itself is more nuanced. Sopinka J. stated for the unanimous Court that:

In *R. v. C. (M.H.)* (1988), 46 C.C.C. (3d) 142 (B.C.C.A.), at p. 155, McEachern C.J.B.C. after a review of the authorities stated what I respectfully accept as a correct statement of the law. He said that: "there is a general duty on the part of the Crown to disclose all material it proposes to use at trial and especially all evidence which may assist the accused even if the Crown does not propose to adduce it". This passage was cited with approval by McLachlin J. in her reasons on behalf of the Court ([1991] 1 S.C.R. 763). She went on to add: "This Court has previously stated that the Crown is under a duty at common law to disclose to the defence all material evidence whether favourable to the accused or not" (p. 774).

As indicated earlier, however, this obligation to disclose is not absolute. It is subject to the discretion of counsel for the Crown. This discretion extends both to the withholding of information and to the timing of disclosure. For example, counsel for the Crown has a duty to respect the rules of privilege. In the case of informers the Crown has a duty to protect their identity. In some cases serious prejudice or even harm may result to a person who has supplied evidence or information to the investigation. While it is a harsh reality of justice that ultimately any person with relevant evidence must appear to testify, the discretion extends to the timing and manner of disclosure in such circumstances. Discretion must also be exercised with respect to the relevance of information. While the Crown must err on the side of inclusion, it need not produce what is clearly irrelevant....

The initial obligation to separate “the wheat from the chaff” must therefore rest with Crown counsel. There may also be situations in which early disclosure may impede completion of an investigation. Delayed disclosure on this account is not to be encouraged and should be rare. Completion of the investigation before proceeding with the prosecution of a charge or charges is very much within the control of the Crown. Nevertheless, it is not always possible to predict events which may require an investigation to be re-opened and the Crown must have some discretion to delay disclosure in these circumstances.²⁵³

Although all material evidence and information should be disclosed, the Crown has the ability, and indeed the obligation, not to disclose “what is clearly irrelevant.” The Crown’s discretion with respect to not disclosing irrelevant information, not disclosing information such as an informer’s identity covered by the law of privilege, and delaying disclosure for reasons such as witness safety or an ongoing investigation is reviewable by the trial judge.

1. The Scope of the Right to Disclosure

As examined in the first part of this study, the Court’s decision in *Stinchcombe* raised considerable concerns that any CSIS information that was given to the police might be subject to disclosure obligations. It is, however, important to recall that *Stinchcombe* contemplated that only evidence that was relevant to the case and the accused’s right to full answer and defence would be subject to disclosure. The Crown has a reviewable discretion not to disclose irrelevant or privileged evidence and to delay disclosure for important reasons such as witness safety or ongoing investigations. It is important that the police and security intelligence agencies understand the precise demands of *Stinchcombe* and that they neither over-estimate nor under-estimate its requirements.²⁵⁴ Misunderstandings of *Stinchcombe* may be in part related to the fact that its standards have yet to be codified in accessible legislation.

²⁵³ [1991] 3 S.C.R. 326

²⁵⁴ For suggestions that the Attorney General of Canada may have overestimated *Stinchcombe* disclosure requirements see *Canada v. Khawaja* 2007 FC 490 revd on other grounds 2007 FCA 342 *Canada v. Khawaja* 2008 FC 560 holding that general analytic reports, administrative material and correspondence with foreign agencies held by the RCMP was not relevant to the accused under the *Stinchcombe* standard in the course of s.38 proceedings. These cases are discussed infra Part VI.

In the years immediately after *Stinchcombe*, the Court addressed, in a number of cases, the question of what evidence was relevant and would have to be disclosed. In a 1993 case, *R. v. Egger*,²⁵⁵ Justice Sopinka stated:

One measure of the relevance of information in the Crown's hands is its usefulness to the defence: if it is of some use, it is relevant and should be disclosed -- *Stinchcombe, supra*, at p. 345. This requires a determination by the reviewing judge that production of the information can reasonably be used by the accused either in meeting the case for the Crown, advancing a defence or otherwise in making a decision which may affect the conduct of the defence such as, for example, whether to call evidence.

Evidence that cannot reasonably be used by the accused is not subject to *Stinchcombe* disclosure obligations.

In 1995, the Court returned to the issue of the breadth of *Stinchcombe* disclosure obligations in *R. v. Chaplin*.²⁵⁶ This case is of particular relevance with respect to concerns that a wide range of intelligence in the hands of the police or prosecutor would have to be disclosed. The accused was subject to a Criminal Code wiretap that was disclosed to him, but further requested to know whether he had been named as a primary or second target in any other wiretaps between 1988 and 1992. The Crown replied that there were no wiretaps "pertaining to this particular investigation during the time period in question".²⁵⁷ The Crown, however, refused to confirm or deny the existence of any other wiretap involving the accused during the time. The unanimous Court dismissed the accused's appeal on the basis that the accused had not established a sufficient basis for further disclosure. Sopinka J. concluded that "once the Crown alleges that it has fulfilled its obligation to produce it cannot be required to justify the non-disclosure of material the existence of which it is unaware or denies. Before anything further is required of the Crown, therefore, the defence must establish a basis which could enable the presiding judge to conclude that there is in existence further material which is potentially relevant. Relevance means that there is a reasonable possibility of being useful to the accused in making full answer and defence."²⁵⁸ He added that:

²⁵⁵ [1993] 2 S.C.R. 451

²⁵⁶ [1995] 1 S.C.R. 727

²⁵⁷ *ibid* at para 5.

²⁵⁸ *ibid* at para 30.

the requirement that the defence provide a basis for its demand for further production serves to preclude speculative, fanciful, disruptive, unmeritorious, obstructive and time-consuming disclosure requests. In cases involving wiretaps, such as this appeal, this is particularly important. Fishing expeditions and conjecture must be separated from legitimate requests for disclosure. Routine disclosure of the existence of wiretaps in relation to a particular accused who has been charged, but who is the subject of wiretaps for ongoing criminal investigations in relation to other suspected offences, would impede the ability of the state to investigate a broad array of sophisticated crimes which are otherwise difficult to detect, such as drug-trafficking, extortion, fraud and insider trading: *R. v. Duarte*, [1990] 1 S.C.R. 30, at p. 44. Wiretaps are generally only effective if their existence is unknown to the persons under investigation. This is implicitly recognized in the secrecy provisions of Part VI of the *Code*, s. 187 and s. 193 which govern until the investigation expires, and the deferred notification of the existence of a wiretap by s. 196.²⁵⁹

The Court distinguished prior cases about the disclosure of wiretaps, such as the *Parmar* case discussed above, on the basis that “the critical fact here is that the Crown stated that no wiretaps had been authorized as part of the investigation leading to the charges.” As such:

Reference to the possible existence of other wiretaps and their connection to the issues in this appeal, however, is purely speculative and mere conjecture. In sum, it is at best, a fishing expedition, and worst, an attempt to determine whether the police have investigated the accused persons in relation to other suspected offences. The appellants provided no basis for believing that there were wiretap authorizations even in existence in relation to investigation of other charges, or that the Crown had relied upon such wiretaps or derivative evidence therefrom in preparing its case. In the circumstances, the Crown was not called upon to justify further the

²⁵⁹ *ibid* at para 32

position it had taken and there was no need for further evidence.²⁶⁰

Chaplin was an early and important indication of the limits of *Stinchcombe*, especially with respect to confidential information that was not relevant to the accused's ability to make full answer and defence in relation to the particular charges faced by the accused. It demonstrated a willingness to shut down disclosure attempts by the accused in situations where the Crown was prepared to certify that all wiretaps in relation to the particular charge had been disclosed, but was not prepared to confirm or deny the existence of wiretaps or other confidential information that was not related to the particular charges.

Chaplin also raises the issue of whether intelligence possessed by CSIS or CSE would be subject to disclosure obligation as evidence that is in the control of the prosecutor. Sopinka J. in *Chaplin* stated that:

This Court has clearly established that the Crown is under a general duty to disclose all information, whether inculpatory or exculpatory, except evidence that is beyond the control of the prosecution, clearly irrelevant, or privileged.²⁶¹

This suggests that *Stinchcombe* might not apply if the prosecution cannot be said to control the information. Foreign intelligence that is not possessed by the prosecution would surely not be controlled by the prosecution. Courts have also been reluctant to hold that provincial prosecutors possess or control information that is held by federal agencies, at least in cases where the federal agency is not a police force and the information cannot be characterized as fruits of the police investigation.²⁶² Whether intelligence possessed by CSIS or CSE would be held to be in the possession of the prosecution would likely depend on the degree of integration of their activities with those of the police. From a functional perspective of preventing terrorism, a high degree of integration would be desirable. A price of this integration, however, may be that more intelligence is subject to disclosure requirements. That said, the Attorney General of Canada still can seek specific non-disclosure orders in particular cases.

²⁶⁰ *ibid* at para 35

²⁶¹ *ibid* at para 21

²⁶² *R. v. Gingras* (1992) 71 C.C.C.(3d) 53 (Alta.C.A.) rejecting request to provincial prosecutor for the federal correctional records of Crown witnesses.

Chaplin suggests that the Crown does not have to disclose intelligence that is not relevant to the particular charges faced by the accused. That said, the breadth of some terrorism offences such as those relating to participation in a terrorist group or facilitation of terrorist activities,²⁶³ or even conspiracy to commit murder charges, may mean that much of the intelligence collected about an accused and his or her associates over an extended period of time might nevertheless be relevant to the wide ranging charges. Nevertheless, *Chaplin* affirms that the choice of particular charges will also affect the breadth of disclosure obligations. Disclosure obligations may be narrowed if the accused faces a charge in relation to a particular act, but they will be broadened if the charge relates to a number of acts over an extended period of time.

The Court revisited the scope of the right to disclosure three years after *Chaplin* in *R. v. Dixon*. In that case, Cory J. commented:

Clearly the threshold requirement for disclosure is set quite low. As a result, a broad range of material, whether exculpatory or inculpatory, is subject to disclosure. See *Stinchcombe, supra*, at p. 343. In particular, “all statements obtained from persons who have provided relevant information to the authorities should be produced notwithstanding that they are not proposed as Crown witnesses” (p. 345). The Crown’s duty to disclose is therefore triggered whenever there is a reasonable possibility of the information being useful to the accused in making full answer and defence.²⁶⁴

The Court suggested that material that must be disclosed under *Stinchcombe* “includes material which may have only marginal value to the ultimate issues at trial.”²⁶⁵ This articulation of *Stinchcombe* stresses the breadth of the disclosure obligations. In a terrorism prosecution, it could be argued that there is a reasonable possibility that much intelligence about an accused or his or her associates could be useful to the accused in making full answer and defence.

²⁶³ Criminal Code ss.83.18 and 83.19.

²⁶⁴ *R. v. Dixon* [1998] 1 S.C.R. 244 at para 21.

²⁶⁵ *ibid* at para 23

2. The Relation Between the Right of Disclosure and the Right to Full Answer and Defence

Even broad understandings of disclosure obligations under *Stinchcombe* stress that the disclosure is a means to an end, and the end is the right of the accused to make full answer and defence and to have a fair trial.

The relation between the right of disclosure and the right to full answer and defence has been discussed in several cases. In *R. v. La*,²⁶⁶ the Court distinguished between the right of disclosure and the right to full answer and defence. The right to disclosure would be violated if there was an inadequate explanation or “unacceptable negligence”²⁶⁷ in making disclosure. In contrast, a violation of the right to full answer and defence required “actual prejudice”²⁶⁸. This latter right would not be violated if “an alternative source of information was available”.²⁶⁹ This opens the important possibility in terrorism prosecutions that there could be alternative sources of information instead of the disclosure of secret intelligence. As will be seen, the idea of adequate substitution of unclassified material for classified material plays an important role in American approaches to establishing a workable relation between intelligence and evidence.

In *R. v. Dixon*²⁷⁰, an unanimous Court distinguished between a right to disclosure that would be violated where the “accused demonstrates a reasonable possibility that the undisclosed information could have been used in meeting the case for the Crown, advancing a defence or otherwise making a decision which could have affected the conduct of the defence” and a right to full answer and defence that would be violated “where an accused demonstrates that there is a reasonable possibility that the non-disclosure affected the outcome at trial or the overall fairness of the trial process.”²⁷¹ Although the right to disclosure has an independent constitutional status under s.7 of the Charter, it is designed to facilitate the right to full answer and defence. The Court has also indicated that there is a temporal dimension to the relation between the two rights. The right to full answer and defence generally becomes relevant when appellate courts review trials, whereas the right to disclosure is concerned with disclosure issues before and during the trial.

²⁶⁶ [1997] 2 S.C.R. 680

²⁶⁷ *Ibid* at para 20

²⁶⁸ *Ibid* at para 25

²⁶⁹ *Ibid* at para 32

²⁷⁰ [1998] 1 S.C.R. 244

²⁷¹ *ibid* at para 34

The Supreme Court revisited the relation between the right to disclosure and the right to full answer and defence in *R. v. Taillefer*; *R. v. Duguay*²⁷². This case involved a large amount of information relating to a murder investigation that was not disclosed to the accused, including inconsistent statements of some Crown witnesses and information that went contrary to the Crown's theory of the case. The Supreme Court affirmed that the accused's right to disclosure was broad and constitutional. LeBel J. stated:

The Crown must disclose all relevant information to the accused, whether inculpatory or exculpatory, subject to the exercise of the Crown's discretion to refuse to disclose information that is privileged or plainly irrelevant. Relevance must be assessed in relation both to the charge itself and to the reasonably possible defences. The relevant information must be disclosed whether or not the Crown intends to introduce it in evidence, before election or plea. Moreover, all statements obtained from persons who have provided relevant information to the authorities should be produced notwithstanding that they are not proposed as Crown witnesses. ... Little information will be exempt from the duty that is imposed on the prosecution to disclose evidence.²⁷³

As in *Dixon*, this case stressed the breadth of the disclosure obligation, albeit with relevance being determined in relation to the charge and reasonably possible defences.

The Court again noted that the violation of the accused's right to disclosure would not necessarily result in a violation of the right to full answer and defence.²⁷⁴ In order to violate the right to full answer and defence, the accused must demonstrate that the failure to make disclosure affected the outcome of the trial or the overall fairness of the trial process. The accused does not have to show that a different verdict was probable, but only a reasonable possibility. This reasonable possibility is assessed in relation to the requirement that guilt be proven beyond a reasonable doubt. The Supreme Court overturned the Quebec Court of Appeal's decision that the right to full answer and defence had not been violated

²⁷² [2003] 3 S.C.R. 307

²⁷³ *ibid* at paras 59-60.

²⁷⁴ *Ibid* at para 71

in this case. The Court of Appeal erred in evaluating the evidence item by item and finding that no item in itself would have affected the verdict. Rather, the focus should be on all the circumstances, both with respect to the outcome of the trial and the overall fairness of the trial process. With respect to the fairness of the trial, courts should consider whether the failure to disclose “deprived the accused of certain evidential or investigative resources. That would be the case, for example, if the undisclosed statement of a witness could reasonably have been used to impeach the credibility of a prosecution witness. The conclusion would necessarily be the same if the prosecution fails to disclose to the defence that there is a witness who could have led to the timely discovery of other witnesses who were useful to the defence.”²⁷⁵ The focus should be on “possible and realistic uses of that evidence by the defence”²⁷⁶.

The Court’s approach in *Taillefer* affirms that the right to disclosure is broad and applies to relevant information including information about witnesses that the Crown does not propose to call. At the same time, the case also stands for the proposition that not every violation of the right to disclosure will violate the right to full answer and defence. The focus in determining whether this later right is violated is on realistic uses of the material by the defence that could affect the outcome or the fairness of the process. Cumulative non-disclosure could violate the right to full answer and defence even though each piece of undisclosed material on its own might not affect the outcome or the fairness of the process.

3. Stinchcombe and the Duty to Preserve Evidence

Soon after *Stinchcombe*, the Supreme Court indicated that a corollary of the right to disclosure of relevant information is a duty of the Crown to preserve such evidence. As will be seen, the destruction of relevant information by CSIS at the Malik and Bagri trial led to a holding that s.7 of the Charter had been violated. The trial judge only avoided fashioning a remedy for such a violation because he acquitted the accused on the merits.

As early as 1993, the Supreme Court indicated that the *Stinchcombe* disclosure obligation would require the Crown to preserve blood samples beyond a minimum period provided in the Criminal Code.²⁷⁷ In 1995,

²⁷⁵ *ibid* at para 84

²⁷⁶ *ibid* at para 99

²⁷⁷ *R. v. Egger* [1993] 2 S.C.R. 451 at 472

the *Stinchcombe* case returned to the Court because the original police notes in that case had been destroyed. In that second *Stinchcombe* case, the Court made clear that the obligation to preserve evidence was not absolute. A satisfactory explanation about why material was not retained might be sufficient to fulfill the Crown's *Stinchcombe* obligations.²⁷⁸ In 1997, the Court elaborated on the proper approach to the preservation of evidence in *R. v. La*, a case in which a tape recorded conversation with a young girl taken in relation to child protection proceedings was not available even though it might have been relevant to the accused in a subsequent sexual assault prosecution in which the girl was the complainant.²⁷⁹ Sopinka J. concluded for the majority of Court:

The right of disclosure would be a hollow one if the Crown were not required to preserve evidence that is known to be relevant. Yet despite the best efforts of the Crown to preserve evidence, owing to the frailties of human nature, evidence will occasionally be lost.... The police cannot be expected to preserve everything that comes into their hands on the off-chance that it will be relevant in the future. In addition, even the loss of relevant evidence will not result in a breach of the duty to disclose if the conduct of the police is reasonable. But as the relevance of the evidence increases, so does the degree of care for its preservation that is expected of the police.²⁸⁰

The Court also left open the possibility that even if the explanation for the loss of evidence was acceptable and the right to disclosure was not violated, "in extraordinary circumstances, the loss of a document may be so prejudicial to the right to make full answer and defence that it impairs the right of an accused to receive a fair trial"²⁸¹. In such cases, a stay of proceedings may be the appropriate remedy. The Court also indicated that the Crown's failure to preserve the relevant evidence might also result in an abuse of process if, for example, material was deliberately destroyed in order to evade disclosure obligations or even, perhaps, if there was "an unacceptable degree of negligent conduct"²⁸² in failing to preserve the evidence.

²⁷⁸ *R. v. Stinchcombe* [1995] 1 S.C.R. 754

²⁷⁹ On the merits the Court found no s.7 violation because of the destruction of the tape, but in large part because the police had recorded four other statements from the girl and she had testified at the preliminary inquiry. *R. v. La* [1997] 2 S.C.R. 680 at paras 32-33.

²⁸⁰ *Ibid* at paras 20-21.

²⁸¹ *Ibid* at para 24

²⁸² *Ibid* at para 22

4. The Application of Stinchcombe Principles in the Air India Prosecution

La played an important role with respect to two separate concessions by the Crown in the Malik and Bagri trial that there had been an unacceptable degree of negligence in the failure to preserve CSIS wiretaps and notes. Without questioning that concession, however, it is important to recognize that the Court's holding in *La* makes some implicit accommodation for the different purposes of intelligence and evidence gathering by stressing that there was no s.7 violation because the destroyed tape recording in that case "was not tape-recorded for the purposes of a criminal investigation" and that the officer "did not turn it over to the police officer who investigated the charges in issue."²⁸³ This suggests some willingness by the Court to accept that disclosure and preservation of evidence obligations do not extend to parallel and separate investigations for different purposes. That said, the Court's decision in *La* suggests that if security intelligence officials shared information with the police, this would be a factor suggesting that the duty to preserve the evidence would apply. It is also possible that the courts could find a violation of the right to full answer and defence, even if the explanation for not retaining intelligence was reasonable and did not violate the right to disclosure.

The *La* case raises the issues of whether some legislative restriction on the duty to preserve evidence is required in the national security context. It could be argued that the potential application of the principle could interfere with the intelligence gathering processes of security intelligence agencies and, especially, in their willingness to share information with police forces, who are clearly subject to the duty to preserve and disclose relevant information. It should be recognized that the duty to preserve evidence and information under *Stinchcombe* cuts both ways. As recognized by Bob Rae in his report, a failure to preserve relevant information can have adverse implications for both the state and the accused. The destruction of CSIS wiretaps and notes in the Air India investigation may have harmed the state's case. At the same time, the destruction of such material may also have deprived the accused of material that would have been helpful in their defence. Because the material has been destroyed, however, we will never know for sure what it may have revealed. This uncertainty suggests that the duty to preserve

²⁸³ *R v. La* at para 29

relevant evidence and information, even as it may apply to terrorism investigations by security intelligence agencies, should not be lightly limited or restricted. The information can be retained even though restrictions are placed on its subsequent distribution for reasons related to privacy or other interests.

An issue that arose at various junctures during the Malik and Bagri prosecution was whether CSIS information was subject to *Stinchcombe* disclosure and retention obligations. Justice Josephson considered the matter in a 2002 motion in relation to the erasure of the CSIS wiretaps. The Crown at first argued that CSIS should be treated as a third party for purposes of disclosure, but in the words of the trial judge “Mr. Code for Mr. Bagri persuasively submits that both law and logic lead to a conclusion that, in the circumstances of this case, CSIS is part of the Crown, and hence subject”²⁸⁴ to *Stinchcombe* obligations. The Crown subsequently conceded that *Stinchcombe* applied to CSIS as a result of a 1987 agreement that the RCMP would have “unfettered access to all relevant information in the files of CSIS...” about the investigation.²⁸⁵ This led Justice Josephson to conclude that “all remaining information in the possession of CSIS is subject to disclosure by the Crown in accordance with the standards set out in *R. v. Stinchcombe*.”²⁸⁶

The 1987 agreement appears to be an exception to the 1986 MOU between CSIS and the RCMP which, as discussed in part 1 of this study, suggests that each agency will not have unfettered access to the files of the other agency. This statement is made not to criticize the 1987 agreement made in the unprecedented context of the Air India investigation, but rather to place Justice Josephson’s conclusion about the applicability of *Stinchcombe* to CSIS in a broader context. Both the Crown’s concession and Justice Josephson’s statements take note of the particular circumstances of the Air India investigation, and leave open the possibility of distinguishing this precedent in future and more routine cases where CSIS carefully controls the information that it discloses to the RCMP.

The issue arose again in 2004 in relation to whether CSIS breached a disclosure obligation in relation to the destruction of the notes and tape recordings of interviews between a CSIS agent and a key Crown witness.

²⁸⁴ *R. v. Malik* [2002] B.C.J. No 3219 at para 9

²⁸⁵ *Ibid* at para 10.

²⁸⁶ *Ibid* at para 14

As in 2002, the Crown conceded that *Stinchcombe* applied to CSIS as a result of the 1987 agreement between CSIS and the RCMP. Even in the absence of such an agreement, Josephson J. concluded:

Despite clear lines of demarcation between the roles of C.S.I.S. and the R.C.M.P., the information obtained from the Witness immediately struck Laurie [the CSIS agent] as being of extreme importance and relevance to the Air India criminal investigation. When, in the course of his information gathering role, he uncovered evidence relevant to that investigation, he was obliged by statute and policy to preserve and pass on that evidence to the R.C.M.P.²⁸⁷

This CSIS interview took place after the bombing of Air India Flight 182. As such, the interview had more obvious evidentiary value than interviews that might have been conducted before an act of terrorism had occurred. After the act of terrorism has occurred, it becomes more difficult to argue that CSIS is discharging its regulatory duties in relation to threats to the security of Canada, as opposed to the determination of some form of penal liability against specific individuals. The Air India investigation was in many ways unique, particularly in the post-bombing period. Justice Josephson's decisions should not stand for the general proposition that CSIS is always subject to *Stinchcombe* disclosure obligations.²⁸⁸ That said, it does suggest that some information held by CSIS in some counter-terrorism investigations may be subject to Charter obligations to preserve and disclose evidence.

Courts of Appeal are divided on the issue of when another government agency becomes subject to *Stinchcombe*. Some Courts of Appeal have held that the Crown should include material held by another Crown agency involved in the investigation,²⁸⁹ while others have held that provincial Crowns in particular cannot disclose material held by federal agencies beyond their control.²⁹⁰ Although some terrorism prosecutions may be conducted by provincial prosecutors, the fact that the federal government can take over such prosecutions and that CSIS works closely

²⁸⁷ *R. v. Malik* [2004] B.C.J. no. 842; 2004 BCSC 554 at para 20

²⁸⁸ A conclusion that CSIS information is subject to *Stinchcombe* disclosure obligations does not automatically require the disclosure of the secret intelligence. The Crown can claim national security confidentiality or other public interest immunities under ss.37 and 38 of the CEA that will be discussed in the next part of this study.

²⁸⁹ *R. v. Arseneault* (1994) 93 C.C.C.(3d) 111 (N.B.C.A.).

²⁹⁰ *R. v. Gingras* (1992) 71 C.C.C.(3d) 53 (Atla.C.A.)

with the police will be relevant factors in deciding whether Crown disclosure in terrorism prosecutions should include relevant CSIS material. Questions may arise in individual cases about whether the Crown has control of intelligence material that may have formed the backdrop for a referral of an investigation from CSIS to the police or about whether a CSIS investigation constitutes fruits of an investigation for the purposes of disclosure.²⁹¹ Nevertheless, information that is possessed in the RCMP's Secure Criminal Investigation System (SCIS), or otherwise possessed by an Integrated National Security Enforcement Team (INSET), composed of the RCMP, municipal, and provincial and other federal agencies including CSIS, would likely be subject to *Stinchcombe* disclosure obligations should the information be relevant in the particular case.²⁹² If the CSIS information is included in the RCMP's SCIS's data base, even if it is subject to restrictions on the use and disclosure of that information, it will be retained until the investigation is marked as concluded and a purge date is provided in accordance with a schedule provide by the Information Management Branch.²⁹³ The public record suggests that the RCMP has taken steps to preserve data in its terrorism investigations in order to satisfy *Stinchcombe* disclosure and retention obligations. As will be seen, the same cannot be said about CSIS.

5. Subsequent Litigation Involving CSIS Destruction of Intelligence

The issue of CSIS's failure to retain and disclose interview notes is the subject of pending litigation in the Supreme Court. The issue arose in security certificate proceedings against Adil Charkaoui. He requested a stay of proceedings on the basis that CSIS did not retain interview notes,

²⁹¹ Higher standards of relevance can be imposed with respect to information that is not possessed or controlled by prosecutors as fruits of investigation or if there is a privacy interest in the material. *R. v. McNeil* (2006) 215 C.C.C.(3d) 22 (Ont.C.A.). See generally David Paciocco "Filling the Seam Between *Stinchcombe* and *O'Connor*: The *McNeil* Disclosure Application" (2007) 53 C.L.Q. 230.

²⁹² Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Public Works and Government Services, 2006) at 102 ff. The Commission reported that information subject to caveats is included in the RCMP's SCIS data base and that the overall approach is of broad inclusion in the data base. This practice is explained in part because of the importance and fluidity of national security investigations and in part because "the RCMP is bound to ensure that all investigation files are complete, in accordance with the standards set by the Supreme Court in the *Stinchcombe* case. Complete files must include both inculpatory and exculpatory information concerning the accused. Information often includes some about individuals with whom the target of the investigation has come into contact. The RCMP has noted in this regard that seemingly benign information can provide a potential accused with alibi evidence." *Ibid* at 109-110.

²⁹³ The Arar commission reported that "given their nature, many national security investigations remain open and files are therefore not subject to purge for a considerable length of the time." *Ibid* at 111. Some major investigations of historical significance such as the Air India investigations are never subject to an automatic destruction of information. *ibid*.

but rather produced a summary of various interviews. Noël J. dismissed this application, largely on the basis that “the interview summaries are of no significance to the foundation of the facts and allegations on which the certificate and the detention are based.”²⁹⁴ He also stated that it was not:

necessary to discuss the role of CSIS in the investigation, other than to say that CSIS is not a police agency and that it is not its role to lay charges. As such, it cannot be subject to the same obligations as those attributed to a police force. Moreover, we are dealing here with immigration law, not the criminal law.²⁹⁵

An appeal by Charkaoui was dismissed by the Federal Court of Appeal, primarily on the grounds that any harm from the destruction of the interview notes was speculative. At the same time, the Court of Appeal considered the government’s defence of the destruction of the interview notes to be less than persuasive:

According to the Ministers, the CSIS duty to confine itself to what is strictly necessary means that once a summary of an interview is written up, it is no longer strictly necessary to preserve notes of the interview and they are then destroyed. This policy, we are told, prevents the accumulation of information on individuals who are not the subject of any suspicion.

On its face, section 12 stipulates that the test of necessity, even strict necessity, applies to the collection of information by investigation or otherwise. If there is a necessity to preserve the information thus collected, it is a practical and not statutory necessity. If the information is not preserved, it cannot then be used for any useful purpose.²⁹⁶

Pelletier J. A. noted that he “must say in passing that I find the justification proffered by the Ministers for this CSIS policy rather unconvincing.”²⁹⁷ It was suggested in the last section, that the “strict necessity” standard in

²⁹⁴ *Re Charkaoui* 2005 FC 149 at para 16

²⁹⁵ *ibid* at para 17.

²⁹⁶ *Re Charkaoui* 2006 FCA 206 at paras 28-29

²⁹⁷ *Ibid* at para 27

s.12 of the CSIS Act should only apply to the collection of intelligence and the destruction of intelligence shortly after its collection because it was not strictly necessary that the intelligence be collected in the first place. It appears, however, that CSIS interprets the standard of “strict necessity” to apply to the retention of intelligence even when that intelligence may become relevant in legal proceedings.

It remains to be seen whether the Supreme Court will address whether and when CSIS has an obligation under s.7 of the Charter to preserve information for disclosure. A conclusion by the Supreme Court that CSIS is subject to retention obligations would likely depend on the fact that the interview was conducted in the context of adversarial proceedings against Charkaoui. In any event, this litigation indicates a continued reluctance by CSIS to take or retain information to evidentiary standards despite the fact that other intelligence agencies, most notably MI5, are prepared to collect to evidential standards in at least some cases.

As suggested above, security intelligence agencies should reconsider the conventional belief that they are unconcerned with evidence in the context of anti-terrorism investigations. The claims that *Stinchcombe* applies to security intelligence agencies become stronger the more their investigations focus on the potential liability of individuals as opposed to general threats to national security. Even if the Federal Court of Appeal’s decision in *Charkaoui* is upheld on grounds related to the particular context of immigration law security certificates, it is clear that the duty to retain information subject to *Stinchcombe* has been recognized under the criminal law, including in the Malik and Bagri terrorism prosecution. As in the Air India investigation, the collection of intelligence to evidentiary standards and the retention of such information could benefit both the crime control interests of the state and the due process rights of the affected individuals.

B) Production and Disclosure of Intelligence as Third Party Records under *R. v. O’Connor*

Even if, on the facts of an individual case, CSIS records are not subject to broad *Stinchcombe* retention and disclosure obligations because they are not in the possession or control of the prosecution, or do not constitute the fruits of the investigation, the accused could still seek production and disclosure of CSIS material under the procedure provided in *R. v.*

O'Connor.²⁹⁸ Although that common law procedure has been displaced by legislation that, as will be discussed in the next section, was held to be constitutional in *R. v. Mills*²⁹⁹, the common law *O'Connor* test still applies to the accused's attempt to obtain access to third party records such as intelligence that do not constitute the private records of complainants in sexual offences.

The *O'Connor* scheme places a higher burden on the accused than *Stinchcombe*. The Court has recognized that:

In the disclosure context, the meaning of “relevance” is expressed in terms of whether the information may be useful to the defence (see *Egger, supra*, at p. 467, and *Chaplin, supra*, at p. 740). In the context of production, the test of relevance should be higher: the presiding judge must be satisfied that there is a reasonable possibility that the information is logically probative to an issue at trial or the competence of a witness to testify. When we speak of relevance to “an issue at trial”, we are referring not only to evidence that may be probative to the material issues in the case (i.e. the unfolding of events) but also to evidence relating to the credibility of witnesses and to the reliability of other evidence in the case.³⁰⁰

Under this test, the accused would have to demonstrate that intelligence held by CSIS was relevant to the alleged facts in a terrorism prosecution or to the credibility of witnesses or the reliability of evidence used in the prosecution. Although this is a higher standard of relevance than *Stinchcombe*, it might often be easily satisfied in the context of a terrorism prosecution where CSIS had the accused or associates of the accused under surveillance. It could also be satisfied in cases where a witness in the prosecution had previously been a CSIS source.

The Court in *O'Connor* was sensitive to the danger of placing the accused in an impossible position of establishing the conclusive relevance of information that he or she had not seen. It also stressed the importance of the accused's right to full answer and defence, and the danger that miscarriages of justice might result from restricting the ability of the

²⁹⁸ *R. v. O'Connor* [1995] 4 S.C.R. 1411

²⁹⁹ *R. v. Mills* [1999] 3 S.C.R. 668

³⁰⁰ *R. v. O'Connor* [1995] 4 S.C.R. 1411 at para 22

accused to call evidence in his or her own defence. It noted that “so important is the societal interest in preventing a miscarriage of justice, that our law requires the state to disclose the identity of an informer in certain circumstances, despite the fact that the revelation may jeopardize the informer’s safety.”³⁰¹

Once the relevance of the requested material to the trial has been established, the common law *O’Connor* procedure then requires the judge to examine the material and consider the case both for and against disclosing the material to the accused. Lamer C.J. and Sopinka J. stated:

...the judge must examine and weigh the salutary and deleterious effects of a production order and determine whether a non-production order would constitute a reasonable limit on the ability of the accused to make full answer and defence. In some cases, it may be possible for the presiding judge to provide a judicial summary of the records to counsel to enable them to assist in determining whether the material should be produced. This, of course, would depend on the specific facts of each particular case.³⁰²

In *O’Connor*, the Court was concerned about the competing rights of the accused to full answer and defence, but also the competing privacy rights of complainants in sexual assault cases. The Court would probably be similarly concerned with the rights of confidential informers who may find their safety threatened by disclosure to the accused. That said, the Court has recognized that even the informer privilege is subject to innocence at stake exceptions.

A court considering a demand for production and disclosure from CSIS under *O’Connor* might also be concerned with how the privacy of third parties might be adversely affected by disclosure of material held by CSIS. Nevertheless, courts have at times been reluctant to apply the full

³⁰¹ *ibid* at paras 18, 25.

³⁰² *Ibid* at para 30. The Court elaborated that “in balancing the competing rights in question, the following factors should be considered: “(1) the extent to which the record is necessary for the accused to make full answer and defence; (2) the probative value of the record in question; (3) the nature and extent of the reasonable expectation of privacy vested in that record; (4) whether production of the record would be premised upon any discriminatory belief or bias” and “(5) the potential prejudice to the complainant’s dignity, privacy or security of the person that would be occasioned by production of the record in question”” *ibid* at para 31 quoting and adopting from the judgment of L’Heureux-Dube J. at para. 156.

O'Connor balancing test to items such as police occurrence reports that were obtained in a manner that implicates the administration of justice as opposed to the private therapy at stake in *O'Connor*.³⁰³ An open question would be whether a judge under *O'Connor* would also balance the state's interest in non-disclosure against the accused's interest in the record. In *O'Connor*, the Court expressed some reluctance to consider the societal interest in encouraging the report of sexual offences in the balancing process. It concluded: "the societal interest is not a paramount consideration in deciding whether the information should be provided. It is, however, a relevant factor which should be taken into account in weighing the competing interests."³⁰⁴ This suggests that courts might consider societal interests in securing intelligence and sharing information that can be used to prevent terrorism when considering an *O'Connor* application for third party records from CSIS or another agency that holds intelligence. There may, however, be a need for Parliament to specify what interests should be considered at this second stage, as was done in the legislation enacted in response to *O'Connor*. If Parliament did so, it would be advisable to be as specific as possible about the harms that might be caused by disclosure and not simply reiterate the idea that disclosure could be injurious to national security, national defence and international relations. These concerns are already well represented in s.38 of the *Canada Evidence Act* which allows the Attorney General of Canada to seek non-disclosure orders.

The second stage of the *O'Connor* test also allows the judge to edit the material to be disclosed so as to preserve as much of the public interest in non-disclosure as possible. In many ways, this resembles and duplicates the process contemplated under ss.37 and 38 of the *Canada Evidence Act*.

C) Summary

Although it excludes information that is clearly not relevant or subject to informer or other privileges, *Stinchcombe* places broad disclosure obligations on the Crown. On the particular facts of the Air India investigation, CSIS was held subject to *Stinchcombe* disclosure obligations, including the duty to preserve evidence. This holding would likely not be applicable to all CSIS activity, but it may be applied to some CSIS counter-terrorism investigations which focus on suspected

³⁰³ *R. v. McNeil* (2006) 215 C.C.C.(3d) 22 (Ont.C.A.). See generally David Paciocco "Filling the Seam Between *Stinchcombe* and *O'Connor*: The *McNeil* Disclosure Application" (2007) 53 C.I.Q. 230.

³⁰⁴ *R. v. O'Connor* [1995] 4 S.C.R. 401 at para 33.

individuals who may well be charged with terrorism offences, and which involve close co-operation with the police. Even when CSIS material is not subject to *Stinchcombe* disclosure requirements, the accused can demand production and disclosure from CSIS of third party records under *O'Connor*.

The broad definition of terrorism offences make it difficult for the Crown to argue that intelligence about the accused or his or her associates is clearly not relevant under *Stinchcombe* or not likely relevant under *O'Connor*. Intelligence that provides general threat assessment or material that deals with administrative matters may, however, not be relevant to the accused and applications by the accused for disclosure or production could be dismissed on that basis. Once the intelligence records were produced before the judge under *O'Connor*, the judge might balance a number of factors in deciding whether they should be disclosed to the accused. Whether this balancing would occur may depend on whether the judge found that the state's interest in non-disclosure of intelligence was as weighty as the privacy interests of complainants in sexual assault cases. The factors that might be included in the balance could include the extent to which access to the intelligence was necessary for the accused to make full answer and defence, its probative value in any trial and the prejudice that disclosure could cause to state interests and privacy. As will be seen in the next section, it could also be possible to enact legislation to govern and restrict applications for the disclosure and production of intelligence under *Stinchcombe* and *O'Connor*. It could also be possible to expand evidentiary privileges as a means of restricting disclosure obligations.

V. Methods of Restricting the Disclosure of Intelligence

There are a variety of means through which Parliament or the courts could place restrictions on the production and disclosure of intelligence. Parliament's legislation in response to *O'Connor* provides some precedent, both for placing legislative restrictions on *Stinchcombe* and on the process for obtaining the production of third party records. Such legislation might attempt to create categories of intelligence that could not be disclosed or establish new procedures and new barriers for accused who seek the disclosure of intelligence. *Mills* suggests that legislative restrictions on disclosure may be held to be consistent with the Charter, even if they result in the Crown having some relevant information that is not disclosed to the accused. It also suggests that Parliament can provide legislative

guidance and procedures to govern production from third parties. Finally, *Stinchcombe* disclosure does not apply to information covered by evidentiary privileges such as police informer privileges. Such privileges could possibly be expanded by legislation.

All of these strategies to restrict the production and disclosure of intelligence would be subject to challenge as violating the accused's rights under the Charter. Even the strongest privileges are subject to innocence at stake exceptions. Restrictions on production and disclosure must still respect the accused's right to full answer and defence. Legislation that restricts the Charter also must survive a test of proportionality. Although various restrictions on *Stinchcombe* and *O'Connor* would be rationally connected to the protection of secrets and the effective operation of security intelligence agencies, the ability to secure non-disclosure orders under ss.37 or 38 of the CEA might constitute less drastic means to secure non-disclosure in the context of particular terrorism prosecutions.

A) Legislative Clarifications of *Stinchcombe*

The Supreme Court decided *Stinchcombe* in the context of reform proposals made by both the Law Reform Commission of Canada and the Commission of Inquiry into Donald Marshall's wrongful conviction, that the Criminal Code be amended to specify disclosure obligations. In *Stinchcombe*, the Court also contemplated that judicial rule making power could be used to clarify procedural details and perhaps even the general principles of disclosure. By and large, however, disclosure matters have not been addressed by rules and legislation. Instead they have been worked out after the fact by the decisions by courts in individual cases. Although such an individualized approach allows decisions to be tailored to the facts of individual cases, it also creates a degree of uncertainty about the scope of disclosure obligations. As seen in part one of this study, perceptions that any information that CSIS might share with the police would be subject to disclosure obligations have adversely affected information sharing between CSIS and the RCMP. There have also been perceptions of inconsistency in the manner that *Stinchcombe* disclosure standards have been interpreted by various criminal justice actors. The Attorney General of Canada in at least one current terrorism prosecution seems to have overestimated the demands of *Stinchcombe* and sought non-disclosure orders for material such as administrative memos identifying personnel and general intelligence assessment that have been held not to be relevant material that should even be disclosed to

the accused.³⁰⁵ All of these shortcomings could potentially be addressed by codification and clarification of disclosure standards.

B) Legislative Restrictions on Disclosure and Production under *Stinchcombe* and *O'Connor*

One of the few contexts in which legislation has been enacted to clarify and narrow the broad disclosure and production obligations and rights contemplated in *Stinchcombe* and *O'Connor* involves the disclosure of therapeutic and other confidential records of complainants in sexual assault cases. Most of the controversy over this matter has focused on the production of such records from third parties such as rape crisis centres and doctors, but these cases also involve legislative restrictions on *Stinchcombe* disclosure obligations on material held by the Crown.

In *R. v. O'Connor*,³⁰⁶ a 5:4 majority of the Supreme Court held that *Stinchcombe* disclosure obligations applied to a complainants' private records that were in the possession of the Crown. Lamer C.J. and Sopinka J. concluded that "where the Crown has possession or control of therapeutic records, there is simply no compelling reason to depart from the reasoning in *Stinchcombe*: unless the Crown can prove that the records in question are clearly irrelevant or subject to some form of public interest privilege, the therapeutic records must be disclosed to the defence."³⁰⁷

In 1997, Parliament enacted legislation that imposed a procedure and required the judge to balance the accused's rights against the complainant's privacy and equality rights, as well as the social interests in encouraging reporting of sexual offences, before ordering that a complainant's private records in the possession of the Crown or a third party would be produced to a judge or disclosed to the accused. The accused argued in *R. v. Mills* that this legislation violated s.7 of the Charter by limiting the broad disclosure required under *Stinchcombe*. The majority of the Court rejected this argument. McLachlin and Iacobucci JJ. distinguished *O'Connor* on the basis that it only applied to records where the complainant had waived her privacy rights. The new legislation

³⁰⁵ *Canada v. Khawaja* 2007 FC 490 rev'd on other grounds 2007 FCA 342 *Canada v. Khawaja* 2008 FC 560 holding that general analytic reports, administrative material and correspondence with foreign agencies held by the RCMP was not relevant to the accused under the *Stinchcombe* standard in the course of s.38 proceedings. These cases will be discussed infra Part VI.

³⁰⁶ [1995] 4 S.C.R. 411.

³⁰⁷ *ibid* at para 14; see also para 189 per Cory J.; at para 254 per Major J.

applied in cases where there was no such waiver and “it was therefore open to Parliament to fill this void legislatively. Viewed in this context, s. 278.2(2) ensures that the range of interests triggered by production will be balanced pursuant to the procedure set out in ss. 278.5 and 278.7. The mere fact that this procedure differs from that set out in *Stinchcombe* does not, without more, establish a constitutional violation.”³⁰⁸

The Court also concluded that the accused’s right to full answer and defence is not “automatically breached where he or she is deprived of relevant information. As this Court outlined in *R. v. La*, [1997] 2 S.C.R. 680, at para. 25, where the claim is based on lost evidence, ‘the accused must establish actual prejudice to his or her right to make full answer and defence.’ Other public interests may similarly limit the accused’s ability to gain access to potentially relevant information. This is clear from *Stinchcombe*, *supra*, where this Court held that the Crown’s disclosure obligation is subject to a privilege exception. Similarly, our law has long recognized the importance of protecting the identity of police informers through an informer privilege, subject to the “innocence at stake” exception”³⁰⁹ In short, the Court ruled that it was constitutional for the Crown “to end up with documents that the accused has not seen, as long as the accused can make full answer and defence and the trial is fundamentally fair.”³¹⁰

In *R. v. Mills*, the Court concluded that there were adequate protections for the right to full answer and defence in the legislation in part because the Crown was required to notify the accused of the documents with enough information as to the date and context of the record as to enable the accused to make an argument that access to the document was required for full answer and defence.³¹¹ Chief Justice Lamer dissented on the basis that the legislation required the accused to establish the likely relevance of a document that he had not seen and that a better procedure would be to allow the Crown to establish that the document was not relevant or privileged.³¹²

The Court also upheld Parliament’s restrictions on the *O’Connor* process of allowing the production and disclosure of records held by third parties not subject to *Stinchcombe*. In s.278.3, Parliament provided a list

³⁰⁸ [1999] 3 S.C.R. 668 at para 109.

³⁰⁹ *Ibid* at para 75.

³¹⁰ *Ibid* at para 112.

³¹¹ *Ibid* at para 115

³¹² *ibid* at para 9.

of assertions that would not be sufficient to establish that the record is likely relevant to an issue at trial or to the competence of a witness to testify. In *Mills*³¹³, the Supreme Court upheld this controversial provision, but stressed that in the end the trial judge would decide whether the record should be produced. The Court also upheld the requirement that production must also be “necessary in the interests of justice” under s.278.5(1). It indicated that in close cases, judges should err on the side of examining the document:

It can never be in the interests of justice for an accused to be denied the right to make full answer and defence and, pursuant to s. 278.5(2) the trial judge is merely directed to “consider” and “take into account” the factors and rights listed. Where the record sought can be established as “likely relevant”, the judge must consider the rights and interests of all those affected by production and decide whether it is necessary in the interests of justice that he or she take the next step of viewing the documents. If in doubt, the interests of justice require that the judge take that step.³¹⁴

The Court also upheld the requirement that the judge consider a variety of factors, including social interests, in encouraging the reporting of sexual offences and the privacy and equality rights of the complainant when deciding whether to disclose the third party record to the accused. It concluded:

By giving judges wide discretion to consider a variety of factors and requiring them to make whatever order is necessary in the interest of justice at both stages of an application for production, Parliament has created a scheme that permits judges not only to preserve the complainant’s privacy and equality rights to the maximum extent possible, but also to ensure that the accused has access to the documents required to make full answer and defence.³¹⁵

The Court’s decision in *Mills* provides some precedent for legislation that could attempt to limit disclosure and production of intelligence.

³¹³ [1999] 3 S.C.R. 668 at para 120.

³¹⁴ Ibid at para 138.

³¹⁵ Ibid at para 144.

The applicability of the Court's decision in *Mills* in the national security context is debatable. The Court's approach in *Mills* is premised on the idea that the Court was reconciling the competing Charter rights of the accused and the complainant and that the matter was not being decided under s.1 of the Charter, where the Crown had the burden of justifying limits on Charter rights. It is possible that future courts might distinguish the national security context as one which pits an individual accused against the admittedly weighty interests of the state. The Crown might defend legislative restrictions on *Stinchcombe* or *O'Connor* in terrorism cases on the basis that terrorism itself infringes the Charter right to security, but this would discount the fact that the immediate threat to human security would come from the terrorist and not from the government. At the same time, legislative restrictions on *Stinchcombe* and *O'Connor* in the national security context might, in some respects, be easier to justify than the regime upheld in *Mills* if the judge were to have access to all the information before making decisions about whether it would need to be disclosed.

Much would depend on the precise content of any legislation. One possibility would be to enact legislation that provides that intelligence or information, the disclosure of which could or would harm national security, national defence or international relations, would not be subject to the Crown's disclosure obligation. The only statutory exception would be information that was exculpatory or mitigated the accused's guilt. Such an approach would violate the right to disclosure under s.7 of the Charter. In *Stinchcombe* and subsequent cases, the Court has clearly rejected the idea, found in American constitutional law, that the accused only had a constitutional right to the disclosure of exculpatory evidence. It may be difficult to determine what is exculpatory without full knowledge about the accused's case. It is also possible that such a legislative restriction might be found to violate the right to full answer and defence, given the interpretation provided to that right in the *Taillefer* case discussed above. In other words, there might be a concern that the disclosure of information that is not on its face exculpatory of the accused might nevertheless deprive the accused of evidential or investigative resources that could lead to the impeachment of Crown witnesses or the discovery of witnesses that would be useful to the defence.

A more nuanced legislative restriction on disclosure and production obligations in the national security context might be adapted from the legislative scheme upheld in *Mills*, albeit with due allowance being made

both for the distinct national security context and the fact that the state's interests in protecting secrets, weighty though they are, may be more akin to social interests in encouraging the reporting of sexual assaults than to a complainant's right to privacy and equality. Such an approach could require a judge to consider the harms to various state interests in the production and disclosure of intelligence. It would be advisable for Parliament to be as specific as possible about these harms and not rely on the broad concept of harm to national security, national defence or international relations that can already be protected under s.38 of the CEA. In *Mills*, the Court indicated that it was constitutionally permissible to consider social interests, so long as judicial discretion was preserved "to ensure that the accused has access to the documents required to make full answer and defence."³¹⁶

Judicial discretion in determining the balance of competing interests in disclosure and non-disclosure could be guided by a non-exhaustive list of factors. For example, the exculpatory value of information or the realistic possibility that it would reveal information useful to the accused in making full answer and defence could be listed as a factor favouring disclosure. In contrast, the fact that the material would reveal sensitive investigative techniques, the identity of undercover operatives or confidential informants, the targets of other investigations or internal administrative information about Canadian or foreign security agencies could be listed as factors that favour the non-disclosure of the material to the accused.³¹⁷ In such a manner, Parliament could provide guidance to judges in exercising judicial discretion without usurping their discretion to decide what information must be disclosed to the accused in order to ensure a fair trial and to protect the accused's right to full answer and defence.³¹⁸

As under s.278.7(3) of the Criminal Code, the judge could be empowered to impose conditions on disclosure to the accused in order to protect, to

³¹⁶ Ibid at para 144.

³¹⁷ In *Canada. v. Khawaja* 2007 FC 490 at para 8, Justice Mosley observed that that accused "has made it clear that he is not seeking the disclosure of any information that would reveal sensitive investigative techniques, the identity of any undercover operatives of law enforcement and/or intelligence agencies, or the targets of any other investigations." In addition, he noted that 350 of the 506 documents of which the Crown sought a non-disclosure order under s.38 of the CEA "may be described generally as internal administrative information such as the names, telephone or fax number of agency employees; internal file numbers; or references to the existence or identities of covert officers in Canada or abroad....[the accused] does not seek disclosure of this type of information." Ibid at para 44. In other cases, however, the accused could seek disclosure of such information and argue that it is not clearly irrelevant or privileged.

³¹⁸ An example of such an open ended listing of factors is found in s.276(3) of the Criminal Code governing the admissibility of prior sexual activity by a complainant in a sexual assault case.

the greatest extent possible, the interests of the state in non-disclosure. Conditions could include editing or summarizing the material, ordering that the material not be disclosed except to the accused and kept or viewed at designated secure locations, conditions that no copies of the record be made and that identifying information either be excised or coded to protect the anonymity of intelligence sources and agents.

Such legislation would be challenged under the Charter and it would be likely to be found to violate the accused's right to disclosure as contemplated under *Stinchcombe* to the extent that *Stinchcombe* applied to the intelligence. The legislation could, however, be defended as a reasonable limit on disclosure and production rights; one that is necessary to protect information that if disclosed would affect vital and important interests of the state. The legislation would be likely to be rationally connected to this state objective, but it could be argued that there are more proportionate alternatives for protecting secrets, such as the existing provisions of ss.37 and 38 of the *Canada Evidence Act*. In many ways, restrictions on *Stinchcombe* disclosure and *O'Connor* production obligations in the national security context would serve a similar purpose to s.38 proceedings in the Federal Court.

If the new restrictions on disclosure and production were applied by the trial judge, however, the procedure might have the benefit of not requiring litigation in a separate court and the possibility of interlocutory or pre-trial appeals. In *Mills*, the Supreme Court suggested that early assignment of a trial judge may allow restrictions on production and disclosure to be decided well before trial.³¹⁹ Such a pre-trial procedure is also advisable given the length and complexity of terrorism prosecutions.³²⁰ Such an approach would require that the trial judge have adequate facilities and training with respect to the handling of secret information because he or she would have to examine the material before determining whether its non-disclosure was consistent with the accused's right to full answer and defence and the accused's right to a fair trial. One of the main advantages of this approach would be that it would follow the practice of other countries in allowing criminal trial judges to make decisions about disclosure of secret material.³²¹ In some cases, the trial judge could also re-visit non-disclosure decisions during the trial if the accused's or the state's interests change.

³¹⁹ *R. v. Mills* at para 145.

³²⁰ Bruce MacFarlane "Structural Aspects of Terrorist Trials" in Vol. 3 of the Research Studies.

³²¹ As discussed *infra* part 7.

One goal of legislative restrictions on *Stinchcombe*, or the production of records held by third parties under *O'Connor*, would be to minimize the need to make applications under s.38 for non-disclosure. Another goal would be to respond to concerns that the breadth of *Stinchcombe* and *O'Connor* may have adversely affected relations between the RCMP and CSIS and the passage of secret intelligence to the police. That said, legislative restrictions on disclosure and production are not a panacea. They would be vulnerable to Charter challenge. It is not clear that *Mills* is applicable in the national security context. Even if legislation restricting *Stinchcombe* disclosure requirements or *O'Connor* production requirements was upheld under the Charter, there could be much litigation about the precise meaning of the legislation and its relation to Charter standards.

Although the state's interests in non-disclosure are particularly strong in the national security context, there is also a particular danger that non-disclosure of intelligence relating to the accused, his associates and witnesses in terrorist prosecutions could increase the risk of miscarriages of justice. The non-disclosure of intelligence could also deprive the accused of important resources to challenge the manner in which the state investigated the case or to suggest that there is an innocent explanation for the accused's activities and associations.³²² The non-disclosure of material received from foreign sources might also deprive the accused of credible arguments that a Canadian process had been tainted by abuse committed outside Canada. Legislative restrictions on disclosure or production could add another layer of complexity, delay and adversarial challenge to terrorism prosecutions.

C) Disclosure and the Protection of Informers and Witnesses

Concerns were raised in the Malik and Bagri prosecution about how disclosure obligations interact with the protection of informers and witnesses. As discussed above, it is important to recall that evidentiary privileges were recognized as a legitimate restriction on the right to disclosure under *Stinchcombe*. The most relevant privilege is the police informer privilege, which protects the informer's name and identifying

³²² The RCMP's investigation of Maher Arar reveals some of the dangers of making conclusions about persons on the basis of their associations or their beliefs. On the dangers of tunnel vision see Federal Provincial Task Force on Miscarriages of Justice (2004). On the experience and dangers of miscarriages of justice in terrorism cases see Kent Roach and Gary Trotter "Miscarriages of Justice in the War Against Terror" (2005) 109 Penn State L.Rev. 967.

information from disclosure without the consent of both the informer and the Crown. This privilege is subject only to the exception that the accused's innocence is at stake.³²³ The traditional innocence at stake exception is consistent with the importance given to the accused's right to full answer and defence under the Charter.

In 1994 in the context of disclosure of affidavits in support of a wiretap in a drug prosecution, the Supreme Court recognized a range of public interest considerations that could justify editing and non-disclosure of material in the affidavits. Building on the recognition of the factors considered by Justice Watt in the *Parmar* case and recognized by the Court in the 1990 *Garofoli* case discussed above, Sopinka J. recognized the following public interest factors now codified in the wiretap provisions of the Criminal Code:

- (a) whether the identities of confidential police informants, and consequently their lives and safety, may be compromised, bearing in mind that such disclosure may occur as much by reference to the nature of the information supplied by the confidential source as by the publication of his or her name;
- (b) whether the nature and extent of ongoing law enforcement investigations would thereby be compromised;
- (c) whether disclosure would reveal particular intelligence-gathering techniques thereby endangering those engaged therein and prejudicing future investigation of similar offences and the public interest in law enforcement and crime detection; and
- (d) whether disclosure would prejudice the interests of innocent persons.³²⁴

At the same time, the Court indicated that "disclosure of the full affidavit should be the starting premise". The Court held that the trial judge had erred by editing out material that was no longer confidential, and warned of the danger of requiring the accused "to demonstrate the specific use

³²³ *R. v. Leipert* [1997] 1 S.C.R. 281

³²⁴ *R. v. Durette* [1994] 1 S.C.R. 469 at 495

to which they might put information which they have not even seen.”³²⁵ Three judges in dissent stressed the dangers of disclosure and observed that “police witness programs, which also apply to informers, eloquently speak to the dangers that such people are facing” and that “editing the information relating to wiretap... are part of this effort by society to protect both the identity of informers and police investigation techniques.”³²⁶ One implication of the majority’s approach, however, is that it may not always be possible to provide complete protection for informants through non-disclosure. In such cases, the adequacy and the attractiveness of witness protection programs become even more important. The failure of the informant in the Parmar prosecution to consent to his identity being revealed was ultimately fatal to that prosecution.

The next case study will reveal how the reluctance to disclose the identity of another informer, as well as the failure to disclose dealings between the police and the informer, ultimately led to a stay of proceedings in a case in which two men had originally been convicted, in 1986, of conspiring to blow up another Air India plane.

D) R. v. Khela: A Case Study of the Limits of Police Informer Privilege and the Failure to Make Full Disclosure

In 1986, five Canadian Sikh men alleged to be members of the Babbar Khalsa were charged in Montreal with planning to blow up Air India flight 110, a Boeing 747, from New York to New Delhi on May 30th of that year. Charges were dropped against three of the individuals due to lack of evidence, but two of the men, Santokh Singh Khela and Kashmir Singh Dhillon, were convicted by a judge and jury, after a three week trial in late 1986, of conspiracy to commit murder. The trial featured evidence of how “Billy Joe”, a convicted drug trafficker and long time police informer³²⁷,

³²⁵ *ibid* at 532

³²⁶ *ibid.* See also *Michaud v. Quebec (Attorney General)* [1996] 3 S.C.R. at paras 48ff stressing the need to limit disclosure to protect informers and warning that the release of even an edited wiretap application could “unintentionally reveal the identity of a police informer with potentially fatal consequences.” *Ibid* at para 53. Note that this case did not involve an application by the accused for disclosure. See also *R. v. Pires; R. v. Lising* [2005] 3 S.C.R. 343 at para 36 noting that concern about revealing the identity of informers is a consideration in restricting the ability of the accused to cross-examine on the affidavit in a challenge to a search warrant.

³²⁷ At trial, Constable Jacques Gagne of the Sureté du Québec testified that he had dealt with Billy Joe for 12 years, that he was known only by his code number 86-07, that Billy Joe had been imprisoned in 1980 for drug possession, conspiracy to traffic in narcotics, forcible confinement and use of a firearm and that the police had guaranteed Billy Joe that he would not have to testify and that they also made successful representations to the parole board to secure the release of one of Billy Joe’s friends. He also indicated that the informer had “left town” even though subject to a subpoena for the trial. “Sikhs victims of police trap defence says” *Montreal Gazette* Dec 10, 1986 A11

had introduced the accused to an undercover FBI agent, Frank Miele, who posed as an explosives expert. The trial featured taped recordings of meetings between the men and evidence about the use of code words to disguise the true meaning of their conversations.³²⁸ The two men were subsequently sentenced to life imprisonment.

The two men's appeal to the Quebec Court of Appeal was successful with Proulx J.A. holding for the Court in 1991 that the trial judge had erred in holding that Billy Joe, an informer, was protected by police informer privilege and need not be called as a witness. Billy Joe had numerous dealings with the accused and was reportedly paid \$8000 by the accused. The Crown's position was that the money was paid in relation to the bombing of the Air India aircraft while the defence's position was that the money was paid in relation to a stolen car. Proulx J.A. concluded:

My analysis of the facts described above in relation to the role of the informer and the law applicable in this case bring me to the conclusion that the informer was "a witness to material facts" and "an agent provocateur who went into the field and that it was "most material to the ends of justice" that disclosure of the identity of the informer be ordered.... the testimony of the informer was relevant to (1) the nature of the agreement (2) the lack of agreement (3) the lack of intent (4) the issue of entrapment (under the existing law at the time) and (5) in relation to credibility.... For these reasons, I am of the opinion that the Trial Judge erred in not ordering at the request of the appellants that the Crown disclose (1) the evidence of the informer before the trial (2) the full name and whereabouts of Billy Joe and (3) that the Crown makes Billy Joe available to the appellants.³²⁹

Despite the privilege that protects the identity of police informers, their identity and evidence would have to be disclosed to the accused in cases where they became a material witness or an agent provocateur. In this case, "Billy Joe" was a crucial witness because of his participation in the events. Although Billy Joe's identity must be disclosed to the accused, the Court of Appeal indicated that it would have been possible to have him

³²⁸ "Montreal Sikhs guilty of plot to bomb plane" *Ottawa Citizen* Dec. 24, 1986

³²⁹ *R. v. Khela* (1991) 68 C.C.C.(3d) 81 distinguishing *R. v. Scott* [1990] S.C.R.

testify under an assumed name in a subsequent trial. Even when disclosure is required to protect the accused's right to full answer and defence, some steps can be taken to limit the damage caused by disclosure.

At the start of the second trial in 1992, the accused applied for a stay of proceedings both on the basis that the Crown had failed to meet its disclosure obligation and on the grounds of a violation of a right to a trial in a reasonable time. The Crown disclosed notes from Billy Joe's police handlers and a statement in which Billy Joe had stated: "Of course, it's blowing up airplanes, and the reason I am ready to testify is because I think it's crazy to conspire to blow up airplanes and to kill hundreds of innocent people."³³⁰ This was claimed to be the only statement made by Billy Joe to the police about the conspiracy. A few weeks before the trial was to start, a person claiming to be Billy Joe was presented to the accused's lawyer, but with his head and face disguised. He would only speak French, even though all his previous discussion had been in English, and he refused to provide his real name and gave only his code name. Justice Steinberg found that the Crown had breached the clear disclosure obligations articulated by the Court of Appeal.³³¹ He also found that 28 months of delay could be attributed to the Crown because of problems with transcripts and other matters. Consequently, he found a violation of the right to a trial in a reasonable time under s.11(b) of the Charter and stayed proceedings. He ordered the release of the accused who had been imprisoned since their 1986 arrest.

The Crown successfully appealed to the Quebec Court of Appeal. The Court of Appeal held that s.11(b) did not apply to appellate delay and that the delay in this case did not violate s.7 of the Charter. The Court of Appeal also agreed with the Crown's submission that because of danger to Billy Joe, "who has already been the subject of a first attempted murder", the issue of whether the Crown was required to disclose Billy Joe's name and whereabouts should have been left to the trial judge. Baudouin J.A. stated: "As the Supreme Court wrote in *R. v. Stinchcombe*, supra, the Crown's obligation to disclose the evidence is not absolute and disclosure need not necessarily be made at any particular time."³³² The Court of Appeal concluded that "there was clearly a misunderstanding if not confusion between the Crown and the defence with respect to the disclosure of the evidence before the trial without there being, however, bad faith". The stay of proceedings should be overturned with matters of

³³⁰ *ibid* at 87

³³¹ *R. v. Khela* 1992 Q.J. No. 409.

³³² *R. v. Khela* (1994) 92 C.C.C.(3d) 81 at 88-89 (Que.C.A.)

disclosure and compliance with the first Court of Appeal decision being left to the trial judge who should have “complete knowledge of the facts and in possession of all the necessary information.”³³³

The accused then appealed to the Supreme Court with mixed success. Sopinka and Iacobucci JJ. concluded that:

...it is quite clear that the Crown totally failed to make full disclosure prior to trial in relation to Billy Joe as required by the three elements of Proulx J.A.'s decision. For the first element, the Crown provided no will-say or statements of the informer prior to trial. For the second element, the Crown did not provide Billy Joe's full, real name, and his whereabouts. The final element of Proulx J.A.'s order is the most problematic. This is because the circumstances of the interview may not have been so much dictated by the Crown, but rather by the informant, Billy Joe, himself.

Failure to comply with the obligation to disclose by the Crown could impair the right of the accused to make full answer and defence in breach of s. 7 of the Charter. Steinberg J. directed a stay but relied, at least in part, on the ground of unreasonable delay which we find was in error. On the other hand, we find that the Crown is in breach of its obligation to disclose as determined by Proulx J.A. The terms of disclosure accord with the decision in *Stinchcombe*, *supra*, except that, in ordering that the informant be made available, the judgment is an extension of the obligation resting on the Crown. Crown witnesses, even informants, are not the property of the Crown whom the Crown can control and produce for examination by the defence. The obligation of the Crown does not extend to producing its witnesses for oral discovery. Nevertheless, subject to variation by appropriate proceedings, the judgment of Proulx J.A. was binding on the Crown, and the Court of Appeal (No. 2) erred in remitting the matter to the trial judge to determine *de novo* the terms, content and conditions of disclosure relating to Billy Joe.³³⁴

³³³ *ibid* at 90.

³³⁴ *R. v. Khela* [1995] 4 S.C.R. 201 at paras 17-18.

Although noting that the order to make Billy Joe available for oral discovery went beyond *Stinchcombe*, the Supreme Court did not fault the defence for refusing to proceed with an interview with a masked and uncooperative man whom they doubted was Billy Joe. The Court ordered that, “subject to variation by the trial judge on the basis of new evidence relating to the jeopardy of Billy Joe”, the Crown must disclose “the evidence of the informer before trial” as well as “the full name and whereabouts of Billy Joe before trial”. Alternatively, the Crown could produce Billy Joe for discovery, “ensuring that he will cooperate and answer all proper questions.”³³⁵ Justice L’Heureux-Dube in dissent agreed with the Court of Appeal that the Court of Appeal’s first judgment was not binding on the trial judge or the parties and that disclosure matters, in light of security concerns, should be left to the trial judge. Like the majority at the Supreme Court, she also indicated that the Court of Appeal’s initial discovery order went beyond *Stinchcombe* because “the Crown can only be ordered to produce what it has, and it does not “have” people.”³³⁶

In 1996, the matter went back for a third trial before a judge, who ordered a stay of proceedings on the grounds of failure to make disclosure and abuse of process. Although the Crown had represented, to the second Court of Appeal and the Supreme Court, that Billy Joe’s statement: “Of course, it’s blowing up airplanes, and the reason I am ready to testify is because I think it’s crazy to conspire to blow up airplanes and to kill hundreds of innocent people”, was the sole statement made by Billy Joe in the Crown’s possession, a large amount of other information relating to Billy Joe came to light and led to the eventual stay of proceedings. Some of this material came from a previously sealed wiretap affidavit. Other information was belatedly produced by the police. The material included a seventeen-page statement taken from Billy Joe in March of 1992. That statement “related in some detail “Billy Joe’s” ongoing relationship with persons whom the RCMP suspected of being Sikh extremists and who, in 1986, were under active investigation. It also revealed that, in early 1986, “Billy Joe” had been approached to orchestrate the murder of Tara Singh Hayer, the editor of the Indo-Canadian Times in Burnaby, B.C. In this connection it recounts that “Billy Joe” received a payment of eight thousand dollars for his efforts. That sum, which, according to “Billy Joe”, had nothing whatever to do with the blowing up of an aircraft, was the same payment which constituted one of the underpinnings of the Crown’s case against petitioners in 1986.”³³⁷

³³⁵ Ibid at para 20.

³³⁶ Ibid at para 41.

³³⁷ *R. v. Khela* [1996] Q.J. no 1940 at para 22 reported 39 C.R.R. (2d) 68

The third trial judge, Justice Martin, conducted a thorough inquiry into the investigation in light of the newly disclosed evidence. He noted that the police agreed to deal with Billy Joe, who had acted as an informer in drug cases in the past and who had approached the police with information about a plot to bomb another Air India plane. Billy Joe "made it clear from the beginning however that his co-operation would, under no circumstances, extend to testifying in favour of the prosecution and this condition was apparently accepted."³³⁸ Justice Martin commented that:

To some degree the Crown's position in this matter, at least in the beginning, is understandable. Occurring as they did at the nadir of the investigation into the Air India tragedy the activities of suspected Sikh militants operating in Canada raised urgent and difficult problems for the authorities. The investigation which the police were obliged to undertake was international in scale and multi-faceted in scope. Furthermore the stakes in terms of human life were very high indeed. The information provided by "Billy Joe", while touching only an aspect of the overall investigation, nevertheless raised the awesome and very real spectre of another aircraft and all aboard being blown to smithereens. This, in any event, was the scenario which "Billy Joe" presented to his QPF controller.³³⁹

Justice Martin also observed that "In view of "Billy Joe's" reluctance, his personal unreliability, his refusal to testify, and the certainty, should he do so, of an embarrassing cross-examination aimed at calling into question his motivation and his dubious credibility, it was decided to replace him by inserting into the operation an undercover agent posing as an "explosives expert" from New-York whom "Billy Joe" would pretend to have recruited. A team of operatives from the New York office of the FBI arrived in Montreal including the undercover agent in question. His name was Frank Miele and he was masquerading under the monicker of George Carbone. By moving "Billy Joe" aside the RCMP hoped, I would suppose, to mount the prosecution from behind the respectability of Miele's badge."³⁴⁰

338 *ibid* at para 37

339 *ibid* at para 35

340 *ibid* at para 40

Although Justice Martin recognized that the Crown's approach was motivated by "real urgency"³⁴¹ and was "a considered and deliberate policy rather than a course of action dictated by the whims of one or other of the numerous prosecutors involved"³⁴², he nevertheless held that it was one that "in my view flies in the face of the principles enunciated in *Stinchcombe*."³⁴³ He identified a number of problems with the Crown's approach that were independent of its refusal to disclose the seventeen-page statement taken from Billy Joe. One was the Crown's position that it need not disclose evidence that had been used to obtain wiretap warrants. He stressed that "the mere fact that information is used to obtain an authorization to intercept private communications will not serve to insulate from disclosure that which the Crown would otherwise be obliged to divulge."³⁴⁴ Another problem was the agreement that Billy Joe would not have to testify.³⁴⁵ Although such an agreement might have been motivated by the urgency of the matter, "the Crown however surely knows that the courts will not be bound by such arrangements. In the end they stand to jeopardize if not torpedo the chances of a successful prosecution."³⁴⁶

Billy Joe, acting through counsel, "objected formally to any disclosure of his identity or whereabouts. The written motion was supported by an affidavit and alleged generally that the Crown had undertaken both to protect his identity and not to require that he testify. It was further alleged that he feared for his safety if his identity was disclosed."³⁴⁷ Billy Joe, however, withdrew this application after defence counsel was granted a right to cross-examine him on his affidavit. Billy Joe's real name was subsequently disclosed to the defence counsel, who agreed with Crown counsel and Billy Joe's counsel upon a method of serving a subpoena on Billy Joe.

The fact that after ten years Billy Joe's name was finally disclosed to the accused underlines the importance of effective witness protection programs. Nevertheless, the eventual disclosure of the informer's name did not relieve the Crown of the consequences for its prior disclosure

³⁴¹ *ibid* at para 41

³⁴² *ibid* at para 71

³⁴³ *ibid* at para 71

³⁴⁴ *ibid* at para 46

³⁴⁵ An officer of the Surete du Quebec testified at the original trial that Billy Joe had received a promise from the police that he would not have to testify. "2 Sikhs guilty of conspiring to bomb plane" *Montreal Gazette* Dec 24, 1986 p. A1.

³⁴⁶ *ibid* at para 67

³⁴⁷ *Ibid* at para 71

violations; both with respect to relevant material in its possession, including that used to obtain the wiretap warrants, as well as with respect to the seventeen-page statement taken from Billy Joe. Martin J. concluded that the undisclosed materials “are capable of raising a reasonable doubt. The material may also have been very relevant to the issue of entrapment.”³⁴⁸

Justice Martin concluded that a stay of proceedings was the appropriate remedy for the various disclosure obligations. He noted that the Supreme Court had already indicated that a stay should be entered if the Crown continued to refuse to disclose Billy Joe’s identity or did not make full disclosure in relation to Billy Joe. The fact that the Crown had recently disclosed Billy Joe’s identity did not relieve it of responsibility for the repeated disclosure violations, including the failure to disclose the seventeen-page statement; a failure that had left both the Court of Appeal and the Supreme Court with the false impression that full disclosure had been made. The Crown’s approach to disclosure “bears all the hallmarks of a deliberate policy decision,”³⁴⁹ was “deliberate” and the prejudice to the accused who had served six years in prison was “palpable.”³⁵⁰ Justice Martin concluded:

It may be that some are dissatisfied with the consequences of *Stinchcombe*. They may consider the additional obligations imposed upon the Crown and by ricochet upon its agents to be onerous, burdensome, and unfair. They may consider the very principle upon which *Stinchcombe* is based, namely that the fruits of the investigation are the property of the public rather than the Crown, to be flawed. But *Stinchcombe* as qualified and developed in later cases is the law of the land. The Crown and the agents of the State have no option but to conform to it. If they will not do so of their own volition then the courts have no choice but to enforce conformity. In some exceptional situations that may regrettably lead to a stay of proceedings. This, in my view is one of those “clearest of cases” where in all fairness I have no other option. The proceedings are stained and that stain cannot be expunged.³⁵¹

348 *ibid* at para 45

349 *ibid* at para 90

350 *ibid* at para 88

351 *ibid* at para 93

The Crown unsuccessfully appealed this stay of proceedings to the Court of Appeal. In its third decision in the matter, the Court of Appeal stressed that the decision to stay proceedings must be considered in light of the Supreme Court's clear directions, setting out specific disclosure requirements that would have to be satisfied to avoid a stay, and Martin J's findings that that "the undisclosed new material 'was of vital interest to the defence', or that it 'would have been of considerable value and assistance to the defence . . ." Proulx J.A. concluded: "To put it bluntly, 'enough is enough'".³⁵²

The *Khela* case demonstrates the limits of police informer privilege when the informer becomes a material witness in an alleged terrorist plot. Although the informer privilege can protect certain informers from disclosure under *Stinchcombe*, it will not apply to those such as Billy Joe, who play an active role, or to those who testify at trial. The reluctance to disclose the interview notes with Billy Joe and all related police notes eventually led to a stay of proceedings, even after the Crown and the accused were able to resolve their long standing dispute over the disclosure of Billy Joe's identity.

Terrorist prosecutions may be highly reliant on human sources, who may not always be reliable. Although electronic surveillance has been used in terrorism prosecutions, conspirators may be guarded about what they say in places that may be bugged. An informer can often be the best source of information about the actions and intent of the accused. The state must take care in handling informers and take care not to make promises about non-disclosure or not testifying that cannot be kept. Interviews and arrangements made with informers should also be fully documented and disclosed if required. If, as in the *Parmar* and *Khela* cases, the identity of informers must be disclosed, it is important that adequate and attractive witness protection programs be available. There is no guarantee that informers such as Billy Joe would enter and co-operate with witness protection programs, but such programs should be available should informers have to testify or have to have their identity otherwise be disclosed.

The *Khela* case also demonstrates how disputes over disclosure can prolong a terrorism prosecution. The case was litigated for twelve years, in large part because of the refusal of the Crown to make full disclosure.

³⁵² *R. v. Khela* (1998) 126 C.C.C.(3d) 341 at 345-346 (Que.C.A.)

At one point, the process was held to violate the accuseds' Charter right to a trial in a reasonable time, but this was overturned on appeal.

E) Use of Privileges as a Means to Restrict Disclosure Obligations

As discussed above, evidence that is covered by a privilege is generally not subject to disclosure requirements under *Stinchcombe*. The identity of Billy Joe in the *Khela* case study discussed above would not have had to be disclosed if the courts had determined that it was subject to police informer privilege. The courts held that Billy Joe was no longer protected by police informer privilege because he acted as an active agent in the case. One possible means to restrict disclosure requirements and provide more certainty about their ambit would be to expand existing privileges. As will be seen, however, there are limits to this approach, as even the most sacrosanct privileges are subject to exceptions to ensure fairness to the accused.

1. Expansion of Police Informer Privilege

The police informer privilege could be expanded to make clear that it includes CSIS informers or informers for other foreign security intelligence agencies. Some might even argue that CSIS itself should be treated as a police informer, even though the privilege has traditionally been designed to protect individuals and not entire state organizations from reprisals. The police informer privilege could also be expanded to apply in cases like *Khela* where the informer lost the benefits of the common law privilege by acting as an agent and becoming a material witness. Matters covered by a valid privilege are not subject to the *Stinchcombe* disclosure requirement.

Such an expansion of the police informer privilege would not, however, be absolute. Although the courts zealously guard police informer privilege, they also have always recognized an innocence at stake exception to the privilege. In 1890, it was recognized that "if upon the trial of a prisoner the judge should be of opinion that the disclosure of the name of the informant is necessary or right in order to shew the prisoner's innocence, then one public policy is in conflict with another public policy, and that which says that an innocent man is not to be condemned when his innocence can be proved is the policy that must prevail."³⁵³ In 1997, the Court held that

³⁵³ *Marks v. Beyfus* (1890) 25 Q.B.D. 494 at 498 (C.A.)

the police informer privilege was consistent with the Charter, but only because it accommodated the innocence at stake exception. The Court stated that “to the extent that rules and privileges stand in the way of an innocent person establishing his or her innocence, they must yield to the Charter guarantee of a fair trial.”³⁵⁴ The Court elaborated:

When an accused seeks disclosure of privileged informer information on the basis of the “innocence at stake” exception, the following procedure will apply. First, the accused must show some basis to conclude that without the disclosure sought his or her innocence is at stake. If such a basis is shown, the court may then review the information to determine whether, in fact, the information is necessary to prove the accused’s innocence. If the court concludes that disclosure is necessary, the court should only reveal as much information as is essential to allow proof of innocence. Before disclosing the information to the accused, the Crown should be given the option of staying the proceedings. If the Crown chooses to proceed, disclosure of the information essential to establish innocence may be provided to the accused.³⁵⁵

Although the innocence at stake exception will not lightly be applied, it would be applied more readily if attempts were made to expand the ambit of police informer privilege or to devise a new class of privilege based on concerns that the disclosure of intelligence might harm national security or international relations.

The Supreme Court in *R. v. Scott*, recognized that “if the informer is a material witness to the crime, then his or her identity must be revealed.... An exception should also be made where the informer has acted as *agent provocateur*”.³⁵⁶ This witness/agent exception and the need to reveal the identity of the informer in some search contexts, have recently been affirmed by the Court as valid examples of the innocence at stake exception.³⁵⁷ This would seem to militate against the expansion of police informer privilege to apply to an informer like Billy Joe, who acted as an agent. Even if an

³⁵⁴ *R. v. Leipert* [1997] 1 S.C.R. 281 at para 24.

³⁵⁵ *Ibid* at para 33.

³⁵⁶ *R. v. Scott* [1990] 3 S.C.R. 979

³⁵⁷ *Unnamed Person v. Vancouver Sun* 2007 SCC 43 at para 29.

expanded police informer privilege was accepted, it would still be subject to an innocence at stake exception. It is more likely that innocence will be at stake when the informer is a material witness or an active agent.

2. Creation of a New National Security Class Privilege for Intelligence

Another possibility would be to create by legislation a new privilege for secret intelligence, or perhaps secret intelligence that Canada has received from foreign agencies or from confidential informants. There has been considerable reluctance to create new class claims of privilege. For example, the Court has rejected a class privilege with respect to religious communications.³⁵⁸ It also has rejected a class privilege with respect to private records in sexual assault cases because a class privilege would conflict with the accused's right to full answer and defence.³⁵⁹ Similar concerns would apply to any new class privilege claim based on concerns about the harms to national security and international relations in disclosing intelligence. Some leading commentators doubt whether any new class privilege will be created, and argue that "the self-interest of Ministers of government in asserting a class claim is evident and warrants close scrutiny."³⁶⁰

Any new national security privilege to protect intelligence from disclosure would likely have to be created by statute and carefully tailored to apply to material whose disclosure would be particularly damaging. A class privilege would, however, have the advantage of providing the greatest amount of *ex ante* protection that information covered by the privilege would not be disclosed. Any new national security privilege would have to be subject to the innocence at stake exception to be consistent with the Charter. If a new privilege was held to be less weighty than police informer or solicitor-client privilege, it could also be subject to a broader exception to recognize the accused's right to full answer and defence.

Both the innocence at stake and full answer and defence exceptions to privilege may be particularly broad in terrorism investigations. Terrorism investigations may involve far-reaching questions about the nature of the accused's associations with others within and outside of Canada. In addition, they may rely on human sources who may have been paid or protected by the state or who may be implicated in crimes including the

³⁵⁸ *R. v. Gruenke* [1991] 3 S.C.R. 263

³⁵⁹ *A (L.B.) v. B(A)* [1995] 4 S.C.R. 536

³⁶⁰ John Sopinka et al *The Law of Evidence* (Toronto: Butterworths, 1999) at 15.39.

broad range of terrorism offences. Some of this information might have to be disclosed even if a new privilege was created. It will simply not be possible to return to the pre-1982 days of an absolute privilege on national security grounds.

3. Case-by-Case Privilege to Protect Intelligence

A less drastic alternative to a class privilege to shelter intelligence from disclosure would be a case-by-case privilege. It is possible that such a privilege might apply to information obtained by Canadian security intelligence agencies from foreign agencies and confidential sources on the basis that: 1) there are communications originating in a confidence that they not be disclosed; 2) confidentiality is essential to the full and satisfactory maintenance of the relation between the parties; 3) the relation must be fostered; and 4) the injury caused to the relation must be greater than the benefit of the correct disposal of the litigation.³⁶¹ The problem with such an approach in the context of the criminal trial, however, is the importance of the accused's right to full answer and defence. Even in the private law context, the Court has rejected an all-or-nothing approach to privilege and held that disclosure may be necessary in some cases, even with respect to private records.³⁶² In the context of private records in sexual assault cases, the Supreme Court recognized that a case-by-case privilege would not address the main policy concerns about disclosure. In other words, it would not be possible to provide an absolute assurance to complainants that their private records would never be disclosed. The records could be disclosed if required for a fair trial.³⁶³ A similar conclusion would be reached in the national security context. It would not be possible to assure foreign agencies or CSIS informants that a disclosure order would never be made. As will be seen, in the next section, the Attorney General of Canada already maintains the ability to issue a certificate under s.38(13) of the Canada Evidence Act and/or to drop a prosecution in cases where a court has found disclosure of national security material to be necessary.

³⁶¹ 8 *Wigmore Evidence* (McNaughton Rev. 1961) s 2285

³⁶² "It follows that if the court considering a claim for privilege determines that a particular document or class of documents must be produced to get at the truth and prevent an unjust verdict, it must permit production to the extent required to avoid that result. On the other hand, the need to get at the truth and avoid injustice does not automatically negate the possibility of protection from full disclosure. In some cases, the court may well decide that the truth permits of nothing less than full production." *M (A) v. Ryan* [1997] 1 S.C.R. 157 at para 33. The Court stressed that the case for disclosure would be easier to make in a criminal case where the accused's liberty was at stake. *Ibid* at para 36.

³⁶³ *A (L.B) v. B(A)* [1995] 4 S.C.R. 536 at para 77.

F) Summary

What, if anything, should be done to alter *Stinchcombe* disclosure obligations or *O'Connor* production obligations as they apply to terrorism prosecutions? Ignoring the requirements of *Stinchcombe* is clearly not an option. *Khela* affirms that flagrant disregard of disclosure obligations can lead to stays of proceedings in even the most serious of cases. Evasion of disclosure requirements also increases the risk of wrongful convictions; a risk that may be significant in terrorism prosecutions.

Parliament's legislation in response to *O'Connor* provides some precedent for both placing legislative restrictions on *Stinchcombe* and on *O'Connor* requirements for production and disclosure from third parties. *Mills* suggests that legislative restrictions on disclosure may be held to be consistent with the Charter, even if they result in the Crown having some relevant information that is not disclosed to the accused. In addition, *Mills* suggests that Parliament can place restrictions on production and disclosure of third party records and require judges to consider, in addition to Charter rights, social interests that would be harmed by production or disclosure. At the same time, the Court in *Mills* recognized that the accused should not be placed in the impossible position of having to demonstrate the relevance of information that he had not seen. The Court indicated that the judge should err on the side of production of the documents, even in a context in which Parliament was reconciling the competing Charter rights of the accused and the complainant. Finally, the accused's right to full answer and defence, as defined in *Taillefer*, can be violated by the cumulative effects of non-disclosure, even if no one single piece of non-disclosed information is capable of raising a reasonable doubt as to guilt or casting doubt on the fairness of the trial.

There are reasons to be cautious about relying on Parliamentary attempts to restrict *Stinchcombe* and *O'Connor*. Any such restrictions will attract Charter challenge. There will also be strong arguments that *Mills* should be distinguished because the national security context pits the state against the individual and does not involve a reconciliation of competing Charter rights. The litigation about whether the information falls within legislative restrictions on disclosure and production and whether the legislation is consistent with the Charter's rights of the accused in the particular case may only add more delay to terrorism prosecutions and duplicate the process that is already available and will be discussed in the next section to obtain non-disclosure orders from judges in particular cases.

The creation or expansion of existing privileges may also create problems. Even the strongest privileges, including police informer privilege, are subject to innocence at stake exceptions. Although a broadened police informer or state secrets privilege would be rationally connected to important objectives with respect to the keeping of secrets, it could be found to be a disproportionate restriction on the accused's Charter rights to disclosure and full answer and defence. The courts have refused to allow even the most established and cherished privileges to be absolute. Any privilege must be subject to at least an innocence at stake exception to be consistent with the Charter. Courts could also find that the existing regime under s.38 of the CEA, including the Attorney's General ability to block disclosure under s.38.13, constitutes a less rights restrictive approach to the creation of new privilege. The section 38 procedure allows for a balancing of competing interests in disclosure and secrecy on the facts of the particular case.

The assertion of a case-by-case privilege will require litigation and will not afford certainty to CSIS, its foreign partners or CSIS informers that disclosure will never occur. It may be difficult to determine whether a case-by-case privilege applies without knowing the value of the information in the criminal trial. Any procedure to restrict disclosure or production that is consistent with the right to full answer and defence should require a judge, likely the trial judge, to examine all the relevant material to determine whether it should be disclosed. This may require trial judges to have adequate facilities and training for the handling of secret information. The determination of whether innocence or full answer and defence is at stake is a matter best decided by the trial judge.

Even if legislation restricting disclosure or production or creating a new privilege was upheld under the Charter, there could be much litigation about the precise meaning of the legislation and its relation to Charter standards. Although the state's interests in non-disclosure are particularly strong in the national security context, there is also a particular danger that non-disclosure could increase the risk of miscarriages of justice in terrorism prosecutions. The non-disclosure of even apparently innocuous information about a suspected terrorist cell could deprive the accused of important resources to challenge the manner in which the state investigated the case and its failure to consider alternative understandings of ambiguous events and associations that could point in the direction of the innocence of the accused. Intelligence could also be relevant to the credibility of human sources and informants.

The apparent certainty produced by new legislation in protecting intelligence from disclosure may be more illusory than real. Any procedure to restrict disclosure or production requirements, or to expand privileges, may duplicate and overlap with procedures already available under s.38 of the Canada Evidence Act to obtain non-disclosure orders. Rather than attempting in advance and in the abstract to restrict disclosure and production or to expand privileges, it may be fairer and more efficient to reform existing processes to allow judges to reconcile the competing interests in disclosure and non-disclosure on the facts of the particular case before them.

VI. Judicial Procedures to Obtain Non-Disclosure Orders

This section will examine the ability of the Crown to seek judicial orders authorizing non-disclosure or modified disclosure for reasons relating to the state's interests in national security, national defence, international relations or other specified public interests. The procedures examined in this section allow judges to determine on the basis of the facts of the particular case whether disclosure is required, whereas the techniques of legislative restrictions and privileges examined in the last section attempt to define information that cannot be disclosed in advance and for all cases. The *ex ante* legislative approach discussed in the last section may at first appear to provide greater certainty that intelligence will not be disclosed, but as suggested above, even the most robust privileges and legislative restrictions will be subject to some exceptions to ensure fair treatment of the accused. The techniques examined in this section are tailored to the facts of specific cases.

As will be seen, the procedures used to obtain non-disclosure orders vary considerably depending on the nature of the public interest in non-disclosure that is asserted. Specified public interests in non-disclosure, as well as common law privileges, can be determined by superior court criminal trial judges under s.37 of the CEA. In contrast, national security confidentiality claims under s.38 that the disclosure of information would injure national security, national defence or international relations, must be determined by specially designated Federal Court judges. The trial judge must accept any non-disclosure order by the Federal Court, but also retains the right to order whatever remedy is required to ensure the fairness of the trial. A number of case studies, including the *Kevork* and *Khawaja* terrorism prosecutions as well as the *Ribic* hostage-taking prosecution, will be used to examine the effects of Canada's dual court approach in resolving claims of national security confidentiality.

A) Section 37 of the CEA and Specified Public Interest Immunity

Section 37 of the CEA provides a procedure for a Minister of the federal Crown or another official to apply to a court for an order that a specified public interest justifies non-disclosure or modified disclosure of certain material. Such applications can, in criminal matters, be heard by the superior court trial judge and be subject to appeal to the provincial Court of Appeal and the Supreme Court. This procedure has been used in some cases to protect the identity of police informers and ongoing investigations.

The heart of s.37 is section 37(5) which provides:

If the court having jurisdiction to hear the application concludes that the disclosure of the information to which the objection was made under subsection (1) would encroach upon a specified public interest, but that the public interest in disclosure outweighs in importance the specified public interest, the court may, by order, after considering both the public interest in disclosure and the form of and conditions to disclosure that are most likely to limit any encroachment upon the specified public interest resulting from disclosure, authorize the disclosure, subject to any conditions that the court considers appropriate, of all of the information, a part or summary of the information, or a written admission of facts relating to the information.

This section instructs the court to balance and, to the extent possible, reconcile the public interest in non-disclosure against the public interest in disclosure. It also provides for a flexible range of conditions to be placed on disclosure in order to reconcile the interests in secrecy with the demands of disclosure. The conditions can include partial disclosure, the use of summaries, or admissions of fact. A common feature of modern legislation with respect to secrets is that judges are empowered to formulate creative solutions to reconcile to the greatest extent possible competing interests in secrecy and disclosure.

Although s.37(5) encourages flexibility in reconciling secrecy with disclosure, it also recognizes that restrictions on disclosure may affect the fairness of subsequent trials. Section 37.3 (1) provides:

A judge presiding at a criminal trial or other criminal proceeding may make any order that he or she considers appropriate in the circumstances to protect the right of the accused to a fair trial, as long as that order complies with the terms of any order made under any of subsections 37(4.1) to (6) in relation to that trial or proceeding or any judgment made on appeal of an order made under any of those subsections.

Section 37.3(2) then encourages trial judges to employ remedial creativity and proportionality in fashioning remedies for the protection of fair trials when it provides that the orders that may be made under subsection (1) include, but are not limited to, the following orders:

- (a) an order dismissing specified counts of the indictment or information, or permitting the indictment or information to proceed only in respect of a lesser or included offence;
- (b) an order effecting a stay of the proceedings; and
- (c) an order finding against any party on any issue relating to information the disclosure of which is prohibited

The regime contemplated under s.37 of the CEA contemplates two ways for judges to reconcile state interests in non-disclosure with the accused's interest in disclosure. The first is when the judge who hears the s.37 application has the option of placing conditions on disclosure under s.37(5), including the use of summaries and partial disclosure. The second can occur under s.37.3(2) when the trial judge is encouraged to engage in remedial creativity while protecting the accused's right to a fair trial in light of a non or modified disclosure order. Although a stay of proceedings remains the ultimate remedy that can be used to protect the accused's right to a fair trial, there is also reference to less drastic remedies such as findings against a party, most likely the Crown, or dismissal of parts of the indictment.

A crucial factor in s.37 is that in criminal trials before provincial superior courts a single trial judge can exercise both the flexible range of disclosure orders under s.37(5) and the flexible remedial powers under s.37.3(2). This is a one court approach similar to those used in other democracies with respect to a broad range of state secrets and public interest immunities. It can be contrasted with the two-court structure used under s.38 of the CEA in which the Federal Court imposes restrictions and conditions on disclosure and the criminal trial court can order a range of remedies to protect the fairness of the trial while being bound by the Federal Court's decision about what can be disclosed. The comparative advantages and disadvantages of the one court approach in s.37 and the two-court approach in s.38 will be assessed and evaluated throughout this part of the study.

The procedures used in a s.37 application are flexible. They can involve *in camera* and even *ex parte* procedures when necessary to protect the secrecy of information.³⁶⁴ The range of public interests that can be invoked under s.37 to justify non-disclosure has deliberately been left open-ended. The courts have, in a series of cases, recognized that the protection of police informers can be a legitimate public interest. In *R. v. Archer*³⁶⁵, the Alberta Court of Appeal held that the identity of a police

³⁶⁴ The British Columbia Court of Appeal has indicated: "If an objection is made, and the public interest is specified, then the trial judge may examine or hear the information in circumstances which he considers appropriate, including the absence of the parties, their counsel, and the public. Whether the trial judge does hear or examine the information, or whether he does not, the trial judge may then either uphold the claim of Crown privilege or order the disclosure of the information either with conditions or unconditionally." *R. v. Meuckon* (1990) 57 C.C.C.(3d) 193 at 199-200 (B.C.C.A.). Charron J.A. has also upheld an *ex parte* proceeding, albeit on the basis of the consent of the accused's counsel. She also stated: "In the circumstances of this case, it was open to the applications judge to adopt the procedure that was suggested to him and consented to by all interested parties on the s. 37 application. There is no hard and fast rule on what procedure will be appropriate on this kind of application. Further, given the wide range of information that can form the subject matter of a s. 37 inquiry, it would not be advisable for this court to establish any such rule... The appellant in this case does not take issue with the notion that the applications judge could review the material in private. Indeed, if a review is to take place under s. 37, all the while preserving the secrecy of the information until a determination can be made, some form of privacy is required. The appellant submits, however, and correctly so, that the procedure followed by Watt J. in *Parmar* did not involve any private meeting between the judge, one of the counsel and a police officer as was done in this case. Hence, although the procedure was consented to in first instance, the appellant now takes issue with the fact that the federal Crown and the investigating officer took part in this private review of the material by the applications judge. In my view, and I express this view with the benefit of appellate hindsight, it would have been preferable if the private meeting had been recorded, or better still, if the required assistance had been provided to the applications judge in a manner that did not involve a private meeting. However, I find no reversible error in this case where the procedure was adopted with the express consent of all interested parties" *R. v. Pilotte* (2002) 163 C.C.C.(3d) 225 at paras 52, 59-60 (Ont.C.A.). See also *R. v. Pearson* (2002) 170 C.C.C.(3d) 549 at para 64 (Que.C.A.) holding that the accused can be excluded from s.37 proceedings if "pressing reasons of security and the protection of witnesses so require it."

³⁶⁵ (1989) 47 C.C.C.(3d) 567

informer should be withheld even when the accused sought to challenge the basis for a search warrant. In *R. v. Babes*,³⁶⁶ the Ontario Court of Appeal has also recognized that the need to protect a police informer can be invoked as a public interest for non-disclosure under s.37.

The Ontario Court of Appeal has also held that common law police informer privilege can be asserted at a preliminary inquiry independent of s.37 of the CEA. The Court of Appeal indicated that in most cases at this preliminary stage the informer privilege will be upheld because the accused's innocence is not at stake.³⁶⁷ This procedure may still be useful in cases where a public interest in non-disclosure is invoked at a preliminary inquiry, but s.37(1.1) now provides that an objection to disclosure under s.37(1) displaces the common law procedure. There are efficiency interests in resolving all claims of privilege together. A two year period spent by the Crown on an unsuccessful non-disclosure application under s.37 has been charged against the Crown and resulted in a stay of proceedings because the accused's right to a trial in a reasonable time was violated.³⁶⁸ As discussed in the last section, there may also be a case for codifying the informer privilege in order to increase certainty about when the privilege applies and when it does not.

Section 37 can be used to protect information relating to ongoing police investigations. Such protection may be particularly relevant in terrorism prosecutions where the state continues to investigate other associates of the accused. In *R. v. Trang*³⁶⁹, a judge recognized that public interest privilege could apply to investigative techniques of the police, ongoing police investigations, and material affecting the safety of individuals. Although the judge did not recognize "police intelligence" as a separate

³⁶⁶ (2000) 146 C.C.C.(3d) 465 (Ont.C.A.) leave to appeal denied

³⁶⁷ *R. v. Richards* (1997) 115 C.C.C.(3d) 377

³⁶⁸ *R. v. Sander* (1995) 98 C.C.C.(3d) 564 (B.C.C.A.) In some cases trial proceedings may go on parallel to s.37 proceedings. See R. Hubbard et al *The Law of Privilege* (Aurora: Canada Law Book, 2007) at 3.40.8

³⁶⁹ (2002) 168 C.C.C.(3d) 145 (Alta.Q.B.). See also *R. v. Chan* (2002) 164 C.C.C.(3d) 24 (Alta Q.B.) recognizing similar common law privileges.

form of privilege, he did recognize that it could be protected from disclosure in some cases.³⁷⁰

Section 37 provides a valuable and flexible vehicle for managing the tensions between secrecy and disclosure in a case-by-case fashion. Rather than either refusing disclosure to the accused or the court, as was done in the first *Khela* trial, or attempting to predict and defend through *ex ante* legislation the appropriate range of restrictions on disclosure, s.37 allows the Crown to invoke an open ended range of specified public interests to justify non-disclosure. Section 37 allows judges, including superior court trial judges in terrorism prosecutions, to make case-by-case decisions about disclosure and partial disclosure, including authorizing the use of summaries and admissions as proportionate alternatives to full disclosure. Section 37.1 and 37.2 contemplate appeals to the relevant Court of Appeal and the Supreme Court from determinations under s.37, but there is some precedent for allowing a trial to proceed, if possible, while these separate appeal rights are exercised.³⁷¹

Section 37.3 also allows trial judges to fashion whatever appropriate and just remedy is required to protect the accused's right to a fair trial. Section 37.3 requires the trial judge, when fashioning such remedies, to comply with a non, or partial, disclosure order previously made under s.37. This raises the possibility that trial judges may be unable to revise their previous non-disclosure orders under s.37, even if they conclude later in the proceedings that non-disclosure would adversely affect the right to a fair trial. As will be seen in the next section, judges in other countries have the ability to revise non-disclosure orders in light of developments during the trial. The ability of trial judges to re-visit and revise non-disclosure orders builds an important flexibility into the system that can benefit both

³⁷⁰ Binder J. elaborated: "It seems to me that as a matter of public policy, having regard to the purpose and role law enforcement is intended to provide to society, it is in the public interest that sensitive intelligence information in the possession of the police be protected. I have little doubt that this is presumed to be so, in the minds of the public. However, I am not persuaded that in the context of disclosure, a new "police intelligence" privilege should be recognized. Rather, if protection is to be afforded, it must fall within a more specific category. For example, the items of information contained in such databases, where relevant, may be subject to privilege on a number of grounds such as investigative technique, ongoing investigation, safety of individuals, or internal communications. Likewise, the structure of the database (or aspects thereof) may be subject to privilege on the basis of investigative technique. Information regarding third parties may be privileged on the basis of privacy, which is addressed later on in these Reasons. This is not to say, however, that "police intelligence" may not be accorded privilege status in the future, particularly having regard to the events of September 11th and the possibility arising therefrom of a substantial widening of "police intelligence". As Lamer C.J.C. opined in *Gruenke*, albeit in reference to class communication privilege, policy considerations may dictate the identification of a new class of privilege on a principled basis." Ibid at para 63.

³⁷¹ *R. v. McCulloch* (2001) 151 C.C.C.(3d) 281 (Alta.C.A.); *R. v. Archer* (1989) 47 C.C.C.(3d) 567 (Alta.C.A.).

the accused and the prosecution. The accused could gain disclosure to information that is necessary for a fair trial only because of developments in the criminal trial. The prosecution will often receive the benefit of non-disclosure made early in the trial process because the judge retains the ability to revisit such orders as the trial develops. Even if the judge orders disclosure later in the trial process, the prosecution retains the right to halt the prosecution in order to protect the information from disclosure.

A decision that non-disclosure is not compatible with a fair trial under s.37 could force the prosecution to return to a domestic or foreign intelligence agency and ask them to re-consider whether the information they have provided can be disclosed. The judge's ruling would make it clear that the state was faced with the difficult choice of either dismissing the prosecution or disclosing the secret evidence. In such circumstances, governments will be able to focus on the difficult trade-offs between secrecy and disclosure in the context of the specific case, rather than in the abstract through legislative restrictions or privileges that apply in all cases. The ultimate decision is such a situation about such trade offs would be made by the prosecutor and not by the judge.

B) Section 38 of the CEA and National Security Confidentiality

1. The Procedure under Section 38 of the Canada Evidence Act

Section 38 provides a complex procedure to govern the protection of information that, if disclosed, would harm national security, national defence or international relations. Unlike s.37, all non-disclosure claims under s.38 must be asserted in the Federal Court and this provision can fragment and disrupt criminal trials.

2. Notice Obligations and Disclosure Agreements

Section 38.01 places obligations on all justice system participants, including the accused, to give written notification, as soon as possible, to the Attorney General of Canada of the possibility that they will disclose or seek to call sensitive or potentially injurious information. "Potentially injurious information" is defined as "information of a type that, if it were disclosed to the public, could injure international relations or national defence or national security", and "sensitive information" is defined as "information relating to international relations or national defence or national security that is in the possession of the Government of Canada, whether originating from inside or outside Canada, and is of a type that

the Government of Canada is taking measures to safeguard.” The breadth of these terms may cause unnecessary use of the s.38 procedure. At the same time, it is open to the Attorney General of Canada to avoid litigation by entering into disclosure agreements with the accused. In addition, once notice is received from a party, the Attorney General is required to make a decision with respect to disclosure within ten days.³⁷²

The notification requirement under s.38.01 is designed to give the Attorney General advance notice “to permit the government to take proactive steps in the appropriate circumstances” and to minimize the need for “proceedings to come to a halt while the matter was transferred to the Federal Court for a determination.”³⁷³ As will be seen, this is precisely what happened in the *Ribic* proceedings, to be examined below, leading to the declaration of a mistrial. At the same time, however, “the scheme continues to permit the government to invoke the provisions of the CEA during the course of the hearing.”³⁷⁴ This means that s.38 issues could still arise during a criminal trial if, for example, the Crown makes late disclosure accompanied by a s.38 claim or if an accused who has not given earlier notices proposes to call a witness who would testify about sensitive or potentially injurious information. Denying the accused the right to call a witness with relevant information could violate the accused’s right to full answer and defence. As occurred in *Ribic*, extensive litigation might be necessary in the Federal Court during the middle of a criminal trial.

Under s.38.03, the Attorney General of Canada may “at any time and subject to any conditions that he or she considers appropriate, authorize the disclosure” of information which is prohibited from disclosure under s.38.02 because a notice has been given under s.38.01. Section 38.031 contemplates disclosure agreements among the Attorney General and persons who have given notice under s.38.01.

3. Ex Parte Submissions and Special Advocates

If no disclosure agreement is made between the Attorney General and the accused, a hearing will take place before a specially designated judge of the Federal Court. The process used in s.38 application has been described as follows:

³⁷² CEA s.38.03

³⁷³ Department of Justice Fact Sheet “Amendments to the Canada Evidence Act”

³⁷⁴ Department of Justice Fact Sheet “Amendments to the Canada Evidence Act”

5. The [Attorney General (A.G.)] advises that the procedure that is used in s. 38.04 *Canada Evidence Act* applications follows a number of customary steps, as follows.
6. First, following the issuance of a notice of application pursuant to s. 38.04, the A.G. files a motion for directions pursuant to paragraph 38.04(5) (a) of the *Canada Evidence Act*. In his motion material, the A.G. identifies all parties or witnesses whose interests he believes may be affected by the prohibition of disclosure of information, and may suggest which persons should be formally named as responding parties to the application. The A.G. requests that this portion of the motion for directions be adjudicated in writing.
7. After reading the A.G.'s motion material, the Federal Court will, pursuant to s. 38.04(5)(c) of the *Canada Evidence Act*, designate the responding parties to the application and order the A.G. to provide notice of the application to these persons by effecting service of the notice of application and motion for directions upon them.
8. The Federal Court will then convene a case conference with the parties to the application (i.e., the A.G. and the responding parties) to discuss the remaining issues raised by the A.G.'s motion for directions, including (1) whether it is necessary to hold a hearing with respect to the matter; (2) whether any other persons should be provided with notice of the hearing of the matter; and (3) whether the application should be specially managed with a formal schedule for the remaining procedural steps. These case conferences are confidential and are held *in camera*. The public is denied access to these case conferences and, generally speaking, only the parties to the application, their counsel, the presiding judge and designated Court staff are present.

9. Following adjudication of the motion for directions, a formal schedule is established to prepare the s. 38.04 *Canada Evidence Act* application for hearing. Like ordinary applications before the Federal Court, these schedules contemplate an exchange of affidavit evidence, cross-examinations on affidavits, the preparation of application records (including memoranda of fact and law) and an oral hearing before a designated applications judge. Unlike ordinary applications before the Federal Court, these schedules contemplate that portions of the affidavit evidence, application records and the oral hearings before a designated applications judge will be “*ex parte*” (i.e., only seen and heard by the A.G. and the Court), while others will be “private” (i.e., seen and heard by the parties and the Court, but not available to the public). Indeed, a typical s. 38.04 *Canada Evidence Act* application will have the following steps:
 - (a) the A.G.’s “private” affidavits are served on the responding party and filed with the Court;
 - (b) the responding party’s “private” affidavits are served on the A.G. and filed with the Court;
 - (c) the A.G.’s “*ex parte*” affidavits are filed with the Court;
 - (d) cross-examinations on the parties’ “private” affidavits take place out of court;
 - (e) the A.G.’s “private” application record is served on the responding party and filed with the Court;
 - (f) the A.G.’s “*ex parte*” application record is filed with the Court;
 - (g) the responding party’s “private” application record is filed with the Court; and

- (h) a hearing is convened at which there are both "private" sessions (at which all the parties are present but the public is excluded) and "ex parte" sessions (at which only the A.G. is present).
10. "Private" affidavits are affidavits prepared by a party to the application that are filed and served on the other parties and to which reference can be made at the portions of the hearings at which all parties are present (i.e., the "private" Court sessions). Such affidavits are, however, confidential by virtue of s. 38.12(2) and cannot be disclosed to the general public.
11. The A.G.'s position is that the "private" affidavits produced by him for the purposes of a s. 38.04 *Canada Evidence Act* application attempt to set out, in general terms, the factual and principled justification for protecting the information in issue from public disclosure, that is to say why the disclosure of the information would be injurious to international relations, national defence or national security. The A.G. advises that these "private" affidavits do not detail the information in issue (i.e., the information covered by the Notice), nor do they contain other specific facts that would themselves constitute "sensitive information" or "potentially injurious information". The A.G.'s stated purpose for filing and serving such "private" affidavits is to provide the responding parties seeking disclosure of the information in issue with as much factual material as possible so that they may understand why the A.G. is attempting to protect the information without compromising the information in issue or other sensitive/potentially injurious information regarding the need to protect the information in issue from disclosure.
12. "Ex parte" affidavits are affidavits that are filed by the A.G. and which are not served on the responding party. They are read only by the presiding judge and are only referred to at the *ex parte* portions

of the hearings where the A.G. is present and the responding party is excluded (i.e., the “*ex parte*” Court sessions) pursuant to s. 38.11(2) of the *Canada Evidence Act*.

13. The A.G.’s position is that the “*ex parte*” affidavits produced for the purposes of a s. 38.04 *Canada Evidence Act* application attempt to set out, in specific terms, the factual justification for protecting the information in issue from public disclosure, that is to say why the disclosure of the information would be injurious to international relations, national defence or national security. These affidavits also contain the information in issue that is covered by the Notice.
14. “Private” application records are filed and served on the other parties and reference can be made to these records at the “private” Court sessions. “*Ex parte*” application records filed by the A.G. are not served on the other parties, are read only by the presiding judge and are only referred to at the “*ex parte*” Court sessions pursuant to s. 38.11(2) of the *Canada Evidence Act*.
15. At the “private” Court sessions at which all parties to the application are present, argument is tendered with respect to, *inter alia*, (1) the potential relevance of the information in issue (if the relevance is not conceded by the A.G.), (2) whether disclosure of the information would be injurious to international relations, national defence or national security and (3) whether the public interest in disclosure outweighs in importance the public interest in non-disclosure. On the question of injury, such argument is presented in generalities by the A.G. because he does not wish to risk disclosure of the information in issue or risk compromising other sensitive/potentially injurious information.
16. At the “*ex parte*” Court sessions at which only the A.G. is present, the A.G. provides argument by reference to the “*ex parte*” affidavits with respect to whether

disclosure of the information in issue would be injurious to international relations, national defence or national security. Counsel for the A.G. will be accompanied by the affiants who have sworn such affidavits so that they may be questioned by the presiding designated judge.³⁷⁵

The above process involves case conferences to determine who should receive notice, preparation and cross-examination on private affidavits that are exchanged between the parties and hearings between the parties. In addition, there are *ex parte* affidavits and hearings from which the accused and his lawyer would be excluded. In short, the s.38 procedure of serving private and *ex parte* applications, public hearings and hearing *ex parte* representations from the Attorney General of Canada and perhaps the accused can be complex and time consuming.

It is possible in a criminal case for the accused to make *ex parte* representations to the Federal Court judge. Chief Justice Lutfy has explained: "the accused may wish to make representations to the section 38 judge concerning the importance of disclosing the secret information to assist in defending the criminal charge. In such circumstances, the accused will prefer to make these submissions without disclosing to any other party the substance or detail of the defence in the criminal proceeding."³⁷⁶ The Federal Court of Appeal has recently indicated that "in order to make a meaningful review of the information sought to be disclosed, the judge must be either informed of the intended defence or given worthwhile information in this respect."³⁷⁷

Although the accused can make *ex parte* submissions, the value of these submissions will be limited by the fact that the accused will not have seen the information that is the subject of the dispute. In addition, the accused may not have developed all possible defences until he or she knows the case to meet, closer to the start of the trial.

The ability of the Attorney General to make *ex parte* submissions has been upheld from Charter challenge, but with an indication that security-cleared lawyers could, if necessary, be appointed to provide adversarial challenge. The ability of the Federal Court to appoint a security-cleared

³⁷⁵ *Toronto Star v. Canada* 2007 FC 128 at para 36.

³⁷⁶ *ibid* at para 37.

³⁷⁷ *Canada v. Khawaja* 2007 FCA 342 at para 35.

lawyer under s.38 is not entirely clear.³⁷⁸ The appointment of such lawyers would not be governed by a new law providing for special advocates in security certificate cases.³⁷⁹ A security-cleared lawyer will require time to become familiar with the case and this will likely cause further delay in s.38 proceedings. At the end of the day, the security-cleared lawyer may never be as familiar with the case as the accused's own lawyer. Special advocates may play an important role in providing adversarial challenge to the government's claim of secrecy, but they will have more difficulty protecting the accused's right to full answer and defence, given limitations on the security-cleared lawyer's familiarity with the case and perhaps his or her ability to consult the accused and take instructions from the accused about the secret information. It is also not clear whether the security-cleared lawyer will be able to demand further disclosure or call additional witnesses.³⁸⁰

In *R. v. Malik and Bagri*, the accuseds' defence lawyers were able to examine undisclosed material on an initial undertaking that the information would not be disclosed to their clients. This allowed the lawyers most familiar with the case to determine the relevance and usefulness of the information and then to present focused and informed demands for disclosure.³⁸¹ The alternative under s.38 is that defence lawyers must make broad and un-informed demands for disclosure because they have not seen the information.

4. Reconciling the Interests in Secrecy and Disclosure under Section 38.06

Under s.38.06, the Federal Court judge determines first whether the disputed information would be injurious to international relations, national defence or national security. If not, the information is relevant

³⁷⁸ *Canada. v. Khawaja* 2007 FC 463 aff'd without reference to the ability to appoint security-cleared lawyers 2007 FCA 388. In his concurring judgment, Pelletier J.A. cast doubt on the ability of the court to order that secret information be disclosed to even a security-cleared lawyer when he concluded that under s.38.02 that "the Court could not order and the Attorney General could not be compelled to provide, disclosure of the Secret Information to Mr. Khawaja, or anyone appointed on his behalf in any capacity." Ibid at para 134. Nevertheless, in *Canada (Attorney General) v. Khadr* 2008 FC 46 a security-cleared amicus curiae was appointed in relation to s.38 proceedings in an extradition matter involving allegations of terrorism. Similarly in *Canada (Attorney General) v. Khawaja* 2008 F.C. 560 a security-cleared amicus curiae was appointed and participated in the second round of s.38 litigation in that case.

³⁷⁹ Bill C-3 *An act to amend the Immigration and Refugee Protection Act* S.C. 2008 c.3.

³⁸⁰ Under Bill C-3, any consultation by the security-cleared lawyer with others about the case after the security-cleared lawyer has seen the information would have to be authorized by the judge.

³⁸¹ Michael Code "Problems of Process in Litigating Privilege Claims" in A. Bryant et al eds. *Law Society of Upper Canada Special Lectures The Law of Evidence* (Toronto: Irwin Law, 2004).

can be disclosed to the accused. If the information is injurious, the judge considers the public interest in both disclosure and non-disclosure. The judge also has the option of placing conditions on disclosure, including authorizing the release of only a part or a summary of the information or a written admission of fact relating to the information. The emphasis under this section is on a flexible reconciliation of competing interests in disclosure and secrecy.³⁸²

Section 38(6) defines the harms of disclosure broadly as material whose disclosure “would be injurious to international relations or national defence or national security.” These terms are broad and vague. National security has been defined as meaning “at minimum the preservation in Canada of the Canadian way of life, including the safeguarding of the security of persons, institutions and freedoms.”³⁸³ National defence has been defined to include “all measures taken by a nation to protect itself against its enemies” and “a nation’s military establishment”. International relations “refers to information that if disclosed would be injurious to Canada’s relations with foreign nations.”³⁸⁴

5. Appeals under Section 38

The accused or the Attorney General has the ability under s.38.09 to appeal a decision under s.38.06 to the Federal Court of Appeal. Although an appeal must be brought within 10 days of the order, there are no time limits on when the appeal must be heard or decided. The Federal Court of Appeal’s decision is not necessarily final as the parties have 10 days after its judgment to seek leave to appeal to the Supreme Court. These provisions create a potential for national security confidentiality issues to be litigated all the way to the Supreme Court before a terrorism trial even starts. If national security confidentiality decisions were decided by the trial judge, it would be possible that they could be appealed after a verdict to the provincial Court of Appeal with the other legal decisions made by the trial judge.

³⁸² Section 38(6) provides: “If the judge concludes that the disclosure of the information would be injurious to international relations or national defence or national security but that the public interest in disclosure outweighs in importance the public interest in non-disclosure, the judge may by order, after considering both the public interest in disclosure and the form of and conditions to disclosure that are most likely to limit any injury to international relations or national defence or national security resulting from disclosure, authorize the disclosure, subject to any conditions that the judge considers appropriate, of all of the information, a part or summary of the information, or a written admission of facts relating to the information.”

³⁸³ *Canada v. Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher arar* 2007 FC 766 at para 68.

³⁸⁴ *Ibid* at paras 61-62.

6. Certificates Issued by the Attorney General to Prevent Court Ordered Disclosure

One rationale for the above appeal rights is that the Attorney General should be able to obtain an appeal before information that may harm national security is disclosed to the accused. Nevertheless, the Attorney General of Canada can personally issue a certificate under s.38.13 “that prohibits the disclosure of information in connection with a proceeding for the purpose of protecting information obtained in confidence from, or in relation to, a foreign entity... or for the purpose of protecting national defence or national security. The certificate may only be issued after an order or decision that would result in the disclosure of the information to be subject to the certificate has been made under this or any other Act of Parliament.” The issue of such a certificate prohibits disclosure, but can be reviewed by a single judge of the Federal Court of Appeal. The reviewing judge can only vary the certificate if he or she determines that “none of the information subject to the certificate relates to information obtained in confidence from, or in relation to, a foreign entity...or to national defence or national security”.³⁸⁵

The ability of the Attorney General to issue a certificate effectively blocking a Federal Court disclosure order under s.38 has been controversial. From the perspective of establishing a workable relation between intelligence and evidence, the Attorney General’s certificate can be seen as the ultimate means of ensuring that commitments given to foreign agencies that intelligence not be disclosed in legal proceedings can be enforced. At the same time, any use of this extraordinary certificate power would likely come with a price. The price might well be that a criminal trial judge could conclude under s.38.14 that a fair trial was no longer possible in light of the executive certificate that effectively reverses a Federal Court order that information should be disclosed to the accused.

7. Powers of Trial Judges to Protect Fair Trials under Section 38.14

Under s.38.14, the trial judge must respect any Federal Court order or Attorney’s General certificate that requires non-disclosure, but can also issue any remedy to protect the accused’s right to a fair trial including a stay of proceedings or all or part of an indictment.

³⁸⁵ CEA s.38.031(9)

Although s.38.14 recognizes a broad remedial discretion, criminal trial judges under s.38.14 have no power to modify the terms of the non, or partial, disclosure order made by the Federal Court judge or an Attorney General's certificate. They also do not have any explicit power to examine the material that is the subject of the Federal Court's non-disclosure order. There is no specific mention in either the Attorney General's power under s.38.03 or the Federal Court judge's power under s.38.06 to allow a trial judge to see information that cannot be disclosed under that section. Although s.38.06(2) gives the Federal Court flexibility in imposing conditions on disclosure orders, it does not contemplate that the Federal Court judge could order undisclosed information be given to the criminal trial judge. The Attorney General might, however, authorize that non-disclosed material be shown to the criminal trial judge under s.38.03, but this power applies to information the disclosure of which is prohibited under s.38.02 and does not explicitly apply to information which has been subject to a judicial non-disclosure order under s.38.06.

Section 38.05 of the CEA contemplates that a trial judge could make a report to a Federal Court hearing a s.38 matter, for example, in the middle of a criminal trial. It does not on its face contemplate a Federal Court judge making a report to a criminal trial judge in order to inform the latter's decision under s.38.14. The Federal Court judge could require the Attorney General of Canada under s.38.07 to notify the trial judge about a non-disclosure order, but this section does not authorize the lifting of the non-disclosure order for the trial judge. A recent decision suggests that the Federal Court judge who makes a s.38 decision could remain seized of the matter during a criminal trial and that the parties could apply for an order clarifying a s.38 ruling.³⁸⁶ The accused, however, would not know what order was subject to a non-disclosure information and as such could not make an informed decision to ask the Federal Court judge to clarify his or her ruling. Although the trial judge's discretion to order remedies to protect the fairness of the trial under s.38.14 is vitally important, the trial judge may well have to make that critical decision without knowledge of what information has been the subject of a non, or partial, disclosure order by the Federal Court under s.38.06.

8. Summary

The two-court approach can be defended as a form of checks and balances that allows the Federal Court to see the secret information, and

³⁸⁶ *Canada (Attorney General) v. Khawaja* 2008 FC 560.

make decisions about non-disclosure, and then allows the trial judge to determine the consequences of non-disclosure independently. It also allows the accused to make *ex parte* submissions to the Federal Court without necessarily disclosing them to the trial judge or the prosecutor. It could even be argued that the two-court process allows the trial judge to be sheltered from knowing about intelligence about the accused that will not be used in trial but is the subject of a non-disclosure order.

Nevertheless, the two-court approach can be criticized on grounds of both efficiency and fairness. The two-court approach is inefficient because it requires separate litigation and appeals in the Federal Court, potentially in the middle of a criminal trial. It creates risks that the trial judge could err on the side of caution in protecting the accused's right to a fair trial and stay proceedings, when such a drastic remedy is not necessary to protect the accused's rights, given the nature of the non-disclosed evidence. Conversely, the two-court structure creates a risk that the trial judge might not be in a position to recognize that the information subject to the non-disclosure order is, in fact, vital to the accused's right to full answer and defence, or even to the accused's innocence. The procedure places the trial judge in the position of having to make very difficult decisions about the future of the criminal trial without having seen the information that is subject to a non-disclosure order.

C. Commentary on Section 38 of the Canada Evidence Act

Although relatively few cases have been decided since the 2001 amendments, section 38 of the CEA has been the subject of much critical commentary. With the exception of some mandatory *in camera* provisions, however, it has so far been upheld as consistent with the Charter.

Stanley Cohen has argued that the 2001 amendments to the CEA "represent an attempt to strike an appropriate balance with regard to the disclosure of important information when national security considerations are involved."³⁸⁷ He noted that the Attorney General's certificate under s.38.13 may be necessary to protect Canada's undertaking to its allies and that s.38.14 provides "a substantial safeguard", including the possibility of a stay of proceedings. He argues that provisions providing for summaries and partial disclosure "sought to promote the ability of affected parties to

³⁸⁷ Stanley Cohen *Privacy, Crime and Terror* (Toronto: Butterworths, 2005) at 307

access and use information relating to international relations or national defence or national security, in a manner consistent with their fair trial rights".³⁸⁸

Hamish Stewart has observed that as a result of the 2001 amendments, s.38 of the CEA is "applicable to a much wider range of information than the traditional doctrine of public interest immunity" because it applies to information that the government has safeguarded whether or not its disclosure would actually be harmful.³⁸⁹ He criticized the bifurcated approach to s.38, especially in criminal cases, on the basis that "the Federal Court judge will make the decision about disclosure without having sat through the trial and without having to decide the remedy (if any) for non-disclosure." Although he recognizes that Federal Court judges have experience in security matters, Professor Stewart argues that they "have no special expertise in the other matters, such as the right to make full answer and defence, against which the security matters will have to be balanced."³⁹⁰

Peter Rosenthal has also criticized the breadth of the information covered by s.38, both in relation to the definition of sensitive information and in relation to information received from foreign entities that may be subject to a s.38.13 certificate.³⁹¹ He notes that the Attorney General has many means to protect information from disclosure. They include proceedings under the common law, under s.37 of the Canada Evidence Act, and under s.38.06 of the Canada Evidence Act and, finally, through the use of a certificate under s.38.13.³⁹² Rosenthal also criticizes the procedures used in s.38 to the extent that they allow *ex parte* proceedings that exclude defence counsel. Finally, he questions whether the provisions for the protection of fair trials will be adequate given that the trial judge making the decision may not always have access to the undisclosed information and the Federal Court judge will not always be able to anticipate defences that might have been raised had the accused had access to the undisclosed evidence.³⁹³

Kathy Grant has criticized the mandatory confidentiality and *ex parte* provisions of s.38. In her view, they mean that "the accused is kept

³⁸⁸ *ibid* at 304

³⁸⁹ Hamish Stewart "Public Interest Immunity After Bill C-36" (2003) 47 C.L.Q. 249 at 252

³⁹⁰ *ibid* at 254.

³⁹¹ Peter Rosenthal "Disclosure to the Defence After September 11: Sections 37 and 38 of the Canada Evidence Act" (2003) 48 C.L.Q. 186 at 191-192

³⁹² *ibid* at 192-193

³⁹³ *ibid* at 196

deliberately in the dark about relevant information. This creates not only a risk of an unfair trial, but the risk that the dangers of an unfair trial will themselves remain secret.”³⁹⁴ As will be seen, both of these features of s.38 have attracted subsequent Charter challenges with mixed success. Jeremy Patrick-Justice has also criticized mandatory publication bans under s.38 and has criticized it as a “slow and unwieldy”³⁹⁵ process that can threaten the completion of trials. He also argues that its scope is overbroad and should only apply to information that, if disclosed, would cause actual harm to national security, national defence or international relations.³⁹⁶

Section 38 has recently been considered by both a Senate and a House of Commons committee conducting a review of the *Anti-terrorism Act*. The House Committee recommended a series of relatively minor amendments, including shortening the length of an Attorney General’s certificate from 15 to 10 years, requiring annual reports of the use of such certificates, and allowing an additional appeal from a judicial review of an Attorney General’s certificate under s.38.13.³⁹⁷ The Senate Committee recommended that a judge reviewing such a s.38.13 certificate be allowed to consider whether the public interest in disclosure outweighs the public interest in non-disclosure.³⁹⁸

Although the ability of the Attorney General to issue a certificate under s.38.13 has attracted considerable attention, there has yet to be any publicly reported use of this power. The ability of the Attorney General to issue a certificate that essentially reverses a court order for disclosure has rightly been regarded as extraordinary, but in some ways it only provides a further gloss on the fundamental dilemma that the government always faces in cases involving sensitive intelligence. The dilemma has been described as the disclose or dismiss dilemma.³⁹⁹ A s.38.13 certificate would not in itself end a prosecution, but such an executive reversal of a court order of disclosure would certainly make it much more likely that a trial judge would stay proceedings under s.38.14 in order to protect the accused’s right to a fair trial. It would also demonstrate that the Attorney General of Canada had personally assumed responsibility for protecting

³⁹⁴ Kathy Grant “The Unjust Impact of Canada’s Anti-Terrorism Act on the Accused’s Right to Full Answer and Defence” (2004) 16 Windsor Review of Legal and Social Issues 137 at 157-158.

³⁹⁵ Jeremy Patrick-Justice “Section 38 and the Open Court Principle” (2005) 54 U.N.B.L.J. 218 at 229.

³⁹⁶ *ibid* at 231

³⁹⁷ *Rights, Limits, Security: A Comprehensive Review of the Anti-Terrorism Act and Related Issues* March, 2007 ch. 6

³⁹⁸ *Ibid* at 62-68.

³⁹⁹ Robert Chesney “The American Experience with Terrorism Prosecutions” in Vol 3 of Research Studies

secret information including promises made to allies that information would not be disclosed.

D) Traditional Cold War Approaches to National Security Confidentiality

There has been a significant evolution in the judicial approach to issues of disclosure and national security. As late as 1982, when the Charter of Rights and Freedoms came into effect, national security confidentiality was seen as a matter of unreviewable executive prerogative. Until it was amended in late 1982, s.41(2) of the Federal Court Act provided an absolute bar on disclosure whenever a federal Minister certified to the Court that disclosure of a document or its contents would be injurious to international relations, national defence or security, or to federal-provincial relations. The Act specifically provided that the court should not examine the document.⁴⁰⁰

In 1982, the *Canada Evidence Act* was amended to allow a specially designated judge of the Federal Court to consider claims that information not be disclosed because it would be injurious to national defence, national security or international relations. This amendment specifically gave the Federal Court judge the ability to examine the material in relation to which a non-disclosure order was sought. Special care was taken to ensure the security of the information that was examined by the specially-designated judges of the Federal Court.

Despite being given the power to review material that was the subject of a national security confidentiality claim, judges were initially reluctant about exercising this right. In 1983, the Federal Court of Appeal unanimously upheld the decision of a judge who denied disclosure of material relating to the RCMP's Secret Service. Former members of the Secret Service, who were charged with theft of the Parti Quebecois's party list, had requested that the material be disclosed and claimed that the material would allow them to argue that they had acted on orders and had a colour of right. Le Dain J. seemed to recognize the potential importance of the material,

⁴⁰⁰ Section 41(2) of the Federal Court Act provided: "(2) When a Minister of the Crown certifies to any court by affidavit that the production or discovery of a document or its contents would be injurious to international relations, national defence or security, or to federal-provincial relations, or that it would disclose a confidence of the Queen's Privy Council for Canada, discovery and production shall be refused without any examination of the document by the court." For background on this provision see Robert Hubbard, Susan Magotiaux and Suzanne Duncan *The Law of Privilege in Canada* (Aurora: Canada Law Book, 2007) at 4.30.

but nevertheless concluded that a judge need not examine it. He stated that he had “reluctantly come to the conclusion that the disclosure of any of the information considered to be sufficient for purposes of the appellants’ defence, even under restrictions of the kind suggested above (assuming that the court, unaided, could determine such sufficiency and the adequacy of the restrictions, of which I have serious doubt) would be likely, for the reasons indicated, in the respondent’s certificate and secret affidavit, to be injurious to national security and international relations, and that such injury would outweigh in importance the relative importance of the disclosure to the appellants’ defence. I thus agree that the information should not be examined and that it should not be disclosed.”⁴⁰¹ In his concurring judgment, Marceau J.A. endorsed the following statement from Chief Justice Thurlow, who had ordered non-disclosure without examining the material, namely that: “it is apparent from the nature of the subject-matter of international relations, national defence and national security that occasions when the importance of the public interest in maintaining immune from disclosure information the disclosure of which would be injurious to them is outweighed by the importance of the public interest in the due administration of justice, even in criminal matters, will be rare.”⁴⁰² He added that it was not necessary to inquire into the degree of harm that disclosure might cause to national security. In his view “to accept that national security and international relations be injured, even to only the slightest extent, in order that such a remote risk of extreme incredulity on the part of 12 members of a jury be avoided, would appear to me, I say it with respect, totally unreasonable.”⁴⁰³ In short, the law has traditionally favoured the state’s interests in keeping secrets over the accused’s need for disclosure.

Traditional attitudes towards national security confidentiality were significantly shaped by Cold War considerations. A good example is an oft-cited case, decided in 1988, with respect to non-disclosure of information about a civil servant who had been denied a security clearance because of his alleged links with Communist groups. In ordering non-disclosure, Addy J. expressed concerns about the mosaic effect, in which: “however innocuous the disclosure of information might appear to be to me, it might in fact prove to be injurious to national security” when received by an ‘informed reader’, that is, a person who is both knowledgeable regarding security matters and is a member of or associated with a group

401 *Re Goguen* (1984) 10 C.C.C.(3d) 492 at 500 (Fed.C.A.).

402 *ibid* at 505

403 *ibid* at 511

which constitutes a threat or potential threat to the security of Canada.”⁴⁰⁴ The assumptions behind the concerns about the mosaic effect should be re-evaluated in light of the changed circumstances. One of the main themes of this study is the need to revisit old assumptions and standard operating procedures with respect to security intelligence in light of the particular challenges of terrorism and the need to prosecute those who would plan or commit acts of terrorist violence.

Addy J. articulated the following concerns justifying non-disclosure for national security reasons:

...generally speaking, such disclosure would either a) identify or tend to identify human sources and technical sources; b) identify or tend to identify past or present individuals or groups who are or are not the subject of investigation; c) identify or tend to identify techniques and methods of operation for the intelligence service; d) identify or tend to identify members of the service; e) jeopardize or tend to jeopardize security of the services telecommunications and cipher systems; f) reveal the intensity of the investigation; g) reveal the degree of success or lack of success of the investigation⁴⁰⁵

The above grounds are very broad. Indeed, there is a danger that they can take on a “boiler-plate” quality that encourages overbroad claims of national security confidentiality. For example, information about members of CSIS or CSIS operations and investigations may not in every case require non-disclosure. What might be required for non-disclosure to protect counter-intelligence operations against hostile states with their own professional intelligence services may not necessarily be required with respect to counter-terrorism operations against loosely connected terrorist cells.

E) Evolving Approaches to National Security Confidentiality and The Dangers of Overclaiming Secrecy

Justice O’Connor, in the report of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, recounted a

⁴⁰⁴ *Henrie v. Canada* (1988) 53 D.L.R.(4th) 568 at 580, 578 affd 88 D.L.R.(4th) 575 (Fed. C.A.).

⁴⁰⁵ *ibid* at 579. For another decision recognizing the mosaic effect see *Ternette v. Canada* [1992] 2 F.C. 75 at paras 35 and 36.

few instances in which the Attorney General of Canada initially made claims of national security confidentiality, but subsequently withdrew them. Although he noted that it may have been understandable for the government to err on the side of caution, Justice O'Connor was critical of the government's approach to national security confidentiality (NSC) claims. He commented that:

...overclaiming exacerbates the transparency and procedural unfairness that inevitably accompany any proceeding that cannot be fully open because of NSC concerns. It also promotes public suspicion and cynicism about legitimate claims by the Government of national security confidentiality....I am raising the issue of the Government's overly broad NSC claims in the hope that the experience in this inquiry may provide some guidance for other proceedings. In legal and administrative proceedings where the Government makes NSC claims over some information, the single most important factor in trying to ensure public accountability and fairness is for the Government to limit from the outset, the breadth of those claims to what is truly necessary. Litigating questionable NSC claims is in nobody's interest. Although government agencies may be tempted to make NSC claims to shield certain information from public scrutiny and avoid potential embarrassment, that temptation should always be resisted.⁴⁰⁶

He raised the "issue of the Government's overly broad NSC claims in the hope that the experience in this inquiry may provide some guidance for other proceedings."⁴⁰⁷

The Federal Court subsequently authorized the disclosure of most of the information that the government had objected to under s.38 of the CEA in the public report prepared by Justice O'Connor. This information included references to the FBI and CIA, references to the use of information obtained from Syria in obtaining a warrant in Canada and provocative statements

⁴⁰⁶ Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar *Report of the Events Relating to Maher Arar Analysis and Recommendations* (Ottawa: Public Works and Government Services) at pp 302, 304.

⁴⁰⁷ Ibid at 304.

made by a senior CSIS official about the intentions of American officials in relation to Maher Arar. Justice Noël held that some of the information that the government had objected to did not even meet the test of injury to national security, national defence or international relations.⁴⁰⁸ This is quite an extraordinary finding, given the deference that is generally paid to the government on whether it has established an injury to national security.⁴⁰⁹

Overbroad national security confidentiality claims are particularly dangerous in terrorism prosecutions because they can delay and fragment terrorism trials through the use of the s.38 procedure. They can create the impression that the accused is being denied access to much vital information and this could even result in a trial judge concluding under s.38.14 that a remedy was required to protect the accused's right to a fair trial. The actual use of this procedure will be examined in three subsequent case studies. At this juncture, however, I will examine the case for revising some national security confidentiality concepts in light of the challenges of terrorism and the dangers of over-use of secrecy claims.

1. Changing Approaches to the Third Party Rule

The third party rule refers to the rule that an agency which receives information subject to a restriction or caveat on its subsequent use should not distribute that information and not use it as evidence in legal proceedings without the consent of the party who sent the information. In terrorism prosecutions, this means that intelligence received from foreign, or even domestic, agencies should not be used in legal proceedings or disclosed to other parties without the consent of the party that sent the information.

Although he stressed the importance of placing restrictions or caveats on information shared with other countries and protesting any breaches of caveats, Justice O'Connor did not see the third party rule as an absolute barrier to the sharing of information. He commented:

⁴⁰⁸ *Canada v. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* 2007 FC 766 at para 91; Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar Addendum (Ottawa: Public Works, 2007).

⁴⁰⁹ Justice Noël for example commented: "It is trite law in Canada, as well as in numerous other common law jurisdictions, that courts should accord deference to decisions of the executive in what concerns matters of national security, national defence and international relations, as the executive is considered to have greater knowledge and expertise in such matters than the courts." *Ibid* at para 46.

Caveats should not be seen as a barrier to information sharing, especially information sharing beyond that contemplated on their face. They can easily provide a clear procedure for seeking amendments or the relaxation of restrictions on the use and further dissemination of information in appropriate cases. This procedure need not be time-consuming or complicated.⁴¹⁰

In a decision in s.38 proceedings in the *Khawaja* terrorism prosecution, Justice Mosley indicated that:

Clearly, the purpose of the third party rule is to protect and promote the exchange of sensitive information between Canada and foreign states or agencies, protecting both the source and content of the information exchanged to achieve that end, the only exception being that Canada is at liberty to release the information and/or acknowledge its source if the consent of the original provider is obtained. In applying this concept to a particular piece of evidence however, the Court must be wary that this concept is not all encompassing. First, there is the question of whether or not Canada has attempted to obtain consent to have the information released. I would agree with the respondent that it is not open to the Attorney General to merely claim that information cannot be disclosed pursuant to the third party rule, if a request for disclosure in some form has not in fact been made to the original foreign source.

Second, as noted by the Court in *Ottawa Citizen*, where a Canadian agency is aware of information prior to having received it from one or more foreign agencies, “the third party rule has no bearing”. In such a case the information should be released unless another valid security interest has been raised: *Ottawa Citizen*, above at para. 66. By way of comparison, it can similarly be argued that where information is found to be publicly available before or

⁴¹⁰ Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar *Report of the Events Relating to Maher Arar Analysis and Recommendations* (Ottawa: Public Works, 2006) at 339.

after it is received from a foreign source, the third party rule equally has no bearing so long as it is the public source that is referenced.⁴¹¹

This approach suggests that the third party rule should not be applied in a mechanical way. Before it is invoked, the government should make good faith and diligent efforts to secure the consent of the third party to the use of the evidence. On the facts of the case, Justice Mosley found a British intelligence agency had refused to consent to the disclosure of information to the accused because of the security situation in that country and an ongoing investigation. At the same time, however, he indicated that a "US agency agreed during the hearing to the disclosure of a significant document that had been previously subject to a restrictive caveat."⁴¹² Although the terrorism context will not alter the basic shape of the third party rule, it should influence the willingness of allies to consent to the disclosure of information for criminal proceedings. Our allies are also struggling with the problems of managing the relation between intelligence and evidence. As examined in the first part of this study, some agencies, such as MI5, have publicized their efforts to collect some intelligence to evidential standards. In addition, the time lag between the collection of the intelligence and its possible disclosure in the trial process may facilitate amendments of caveats to allow disclosure. For example, the completion of a particular terrorism investigation or prosecution may allow allies to agree to the disclosure of information that was originally provided under caveat.

Unfortunately, there are signs of resistance to a modified approach to the third party rule that would require the government to seek the consent of the originating agency before claiming the benefits of the third party rule. In *Canada v. Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar*⁴¹³, Justice Noël describes how an affidavit filed by a person employed by the RCMP claimed that "if the RCMP were to seek consent to disclose the information in this case, the RCMP's commitment to the third party rule may be questioned, as disclosure would be sought for a purpose other than law-enforcement, and therefore outside the general accepted parameters for seeking consent (X (for the RCMP)'s

⁴¹¹ *Canada. v. Khawaja* 2007 FC 490 at paras 145-147. Note that a small part of this decision has been reversed -- but on grounds of factual errors in preparing a schedule, and not on the basis of legal errors. *Canada. v. Khawaja* 2007 FCA 342.

⁴¹² *Ibid* at para 153. See also *Canada v. Khawaja* 2008 F.C. 560 at para 8 indicating that additional information was disclosed when a foreign agency agreed to the disclosure of information that had originally been provided under caveat.

⁴¹³ 2007 FC 766

affidavit, at paragraph 42)."⁴¹⁴ If accepted, such an approach could severely inhibit attempts to obtain consent to allow for the use of intelligence as evidence or as information that could be disclosed to the accused.⁴¹⁵ In my view, a request for consent for disclosure under the third party rule actually affirms Canada's commitment to the third party rule and its requirement for consent for subsequent disclosure of information. The originating agency still retains the right to say no and not amend the caveat that it originally attached to the information.

The third party rule remains a critical component of legitimate claims of national security confidentiality, but it should not be invoked in a mechanical manner. It only applies to information that has been received in confidence from a third party and should not be stretched to apply to information that either was in the public domain or was independently possessed by Canadian agencies, provided that those independent sources of information are used. Canadian agencies should generally seek the consent of the originating agency to the use of information covered by the third party rule, as recommended both by the Arar Commission and by Justice Mosley. Those agencies may refuse consent, but they too are struggling with similar problems in managing the relation between intelligence and evidence with respect to counter-terrorism investigations. Asking for consent under a caveat affirms Canada's commitment to the third party rule, and provides an opportunity for the originating agency to consent to the use or disclosure of intelligence in a terrorism prosecution.

2. Changing Approaches to the Mosaic Effect

The mosaic effect refers to a process in which the disclosure of an apparently innocuous piece of information may have harmful effects because a hostile party can fit the information into a broader mosaic of other information. This concern makes sense in the Cold War context in which a professional intelligence service such as the KGB could systematically monitor disclosures from the West. As suggested above, it makes less sense when the hostile party is a non-state actor, such as terrorist group. Although groups such as Al Qaeda may devote some

⁴¹⁴ *ibid* at para 72.

⁴¹⁵ Justice Noël does not comment directly on this assertion in his public judgment, but he does warn that "care must be taken when considering whether to circumvent the third party rule in what concerns information obtained from our most important allies." *Ibid* at para 80

resources to counter-intelligence, they do not have the resources available to state actors. Many terrorist groups are more loosely organized than Al Qaeda. The mosaic effect is not nearly as pressing in the counter-terrorist context as it was in the Cold War.

Despite the changed context, there is some public evidence that CSIS has continued to place reliance on the mosaic effect in justifying non-disclosure. For example, in his public judgment in the Arar Commission matters, Justice Noel cites a CSIS representative who in his affidavit states that:

... in the hands of an informed reader, seemingly unrelated pieces of information, which may not in and of themselves be particularly sensitive, can be used to develop a more comprehensive picture when compared with information already known by the recipient or available from another source. By fitting the information disclosed by the Service with what is already known, the informed reader can determine far more about the Service's targets and the depth of its knowledge than a document on its face reveals to an uninformed reader. In addition, by having some personal knowledge of the Service's assessments and conclusions on an individual or the depth, or lack, of its information regarding specific threats would alert some persons to the fact that their activities escaped investigation by the Service.⁴¹⁶

What is striking and disturbing about the above statement, is that it could have been written during the height of the Cold War and it provides no specific information about how the mosaic effect might apply in the particular case.

Fortunately, there are signs that courts are starting to taking a harder look at claims by the government that non-disclosure is justified because of concerns about the mosaic effect. For example, Justice Noel concluded, as did Justice Mosley in his *Khawaja* decision, that "by itself the mosaic effect will usually not provide sufficient reason to prevent the disclosure of what would otherwise appear to be an innocuous piece of information. Something further must be asserted as to why that particular piece

⁴¹⁶ quoted *ibid* at para 83

of information should not be disclosed.”⁴¹⁷ Pelletier J.A., however, has stressed that “the difficulty in deciding whether information, apparently innocuous on its face, has value to a hostile observer goes a long way towards explaining Parliament’s decision to authorize *ex parte* submissions by the Attorney General”.⁴¹⁸ In his judgment, concerns about the mosaic effect justify the *ex parte* process under s.38. This is, of course, a slightly different question than whether invocation of the mosaic effect alone should have substantial weight under s.38.06 of the CEA in determining the appropriate balance between secrecy and disclosure.

In my view, both the courts and domestic and foreign security agencies should re-examine old assumptions behind routine invocations of the mosaic effect as a justification for broad claims of secrecy. They should consider the increased likelihood that intelligence about terrorism may have evidentiary value and the decreased likelihood that terrorist groups, as compared to foreign intelligence agencies, may be systematically monitoring all disclosed information. The assumptions behind the concept of the mosaic effect should be re-examined and re-evaluated in the context of counter-terrorism. As has been emphasized throughout this study, the practices of governments and the legal system need to evolve with the increasing importance assigned to counter-terrorism work. Concerns about the mosaic effect may have made sense during the Cold War, but they are a much less powerful justification for secrecy with respect to counter-terrorism prosecutions today.

3. Towards a More Disciplined Harm-Based Approach to Non-Disclosure

The Senate Committee that reviewed the Anti-Terrorism Act recommended that the terms “potentially injurious information”, “sensitive information”, and the reference to harm to “international relations” in s.38, be amended to specify the way in which information covered by s.38 would harm legitimate interests.⁴¹⁹ This recommendation could also be extended to the references to national security and national defence in s.38. In his s.38 decision with respect to the Arar Commission, Justice Noël attempted the difficult task of defining the operative terms of s.38 application. He suggested that national security “means at minimum the preservation in Canada of the Canadian way of life, including the safeguarding of the

⁴¹⁷ *ibid* at para 84. See also *R. v. Khawaja* 2007 FC 490 at para 136.

⁴¹⁸ *Khawaja v. Attorney General of Canada* 2007 FCA 388 at para 124.

⁴¹⁹ *Fundamental Justice In Extraordinary Times: The Report of the Senate Committee on the Anti-Terrorism Act* February, 2007 at 64

security of persons, institutions and freedoms.”⁴²⁰ National defence includes “all measures taken by a nation to protect itself against its enemies” and “a nation’s military establishment.”⁴²¹ Finally, international relations “refers to information that if disclosed would be injurious to Canada’s relations with foreign nations.”⁴²² Although the attempt at definition is admirable, the result is not satisfactory. It is difficult to imagine broader and vaguer statutory terms than national security⁴²³ or international relations. Alas, these terms seem to have become even broader in the process of judicial interpretation and definition. The root problem is the vagueness of the statutory terms. In the investigative hearing cases, the Supreme Court pointedly refused to accept the government’s argument that the purpose of the ATA was to protect “national security”, in part because of a concern about the “rhetorical urgency”⁴²⁴ of the broad term.

There is a need to re-think “boiler-plate” claims of secrecy in light of the disclosure and evidentiary demands of terrorism investigations and prosecutions. In one recent case, the Attorney General of Canada justified its s.38 on the following basis:

The applicant asserts that CSIS has the following general concerns in relation to national security which are engaged by the potential release of information collected during the course of its investigations in that it may:

- a) identify or tend to identify Service employees or internal procedures and administrative methodology of the Service, such as names and file numbers;
- b) identify or tend to identify investigative techniques and methods of operation utilized by the Service;
- c) identify or tend to identify Service interest in individuals, groups or issues, including the existence or absence of past or present files or investigations, the intensity of investigations, or the degree or lack of success of investigations;

420 *Canada v. Commission of Inquiry* 2007 FC 766 at para 68

421 *ibid* at para 62

422 *ibid* at para 61

423 Craig Forcese “Through a Glass Darkly: The Role and Review of ‘National Security’ Concepts in Canadian Law” (2006) 43 *Alta.L.Rev.* 963.

424 *Re Section 83.28 of the Criminal Code* [2004] 2 S.C.R. 248 at para 39.

d) identify or tend to identify human sources of information for the Service or the content of information provided by a human source;

e) identify or tend to identify relationships that the Service maintains with foreign security and intelligence agencies and would disclose information received in confidence from such sources; and

f) identify or tend to identify information concerning the telecommunication system utilized by the Service.⁴²⁵

Justice Mosley described the above as “a useful classification scheme with respect to the grounds advanced by the Attorney General to justify non-disclosure for all of the redacted material including that from other agencies and I have relied upon it generally in assessing the information.”⁴²⁶ Nevertheless, there are grounds to be cautious about such generic claims about the need for secrecy. Although the identity of some employees, some investigative techniques and some telecommunications techniques should be kept secret, this is not necessarily true in all cases. Although it is important that ongoing investigations be kept secret, it may be difficult to justify secrecy with respect to all the individuals, groups or issues that may attract the attention of CSIS. In this respect, it may be helpful to distinguish between general strategic intelligence and tactical intelligence in relations to specific targets. There are dangers in conflating the need to protect vulnerable human sources and to protect relationships with foreign agencies that may be embarrassing or the subject of legitimate criticism. Similarly, the need to respect a caveat is a more compelling reason for secrecy than the generic need to protect information that identifies relationships with foreign security and intelligence agencies. In general, there is a need to be as specific as possible about the precise harms of disclosure of secret information.

There are some very good reasons to protect secrets, including threats to the safety of informants, threats to ongoing investigations and promises made to our allies. These reasons, however, may be lost in references to the vague generalities of national security, national defence and

⁴²⁵ *R. v. Khawaja* 2007 FC 490 at para 132 rev'd in part on other grounds 2007 FCA 388

⁴²⁶ *ibid* at para 133

threats to international relations. The breadth of the definitions may play a role in encouraging the government to overclaim national security confidentiality. In light of both the overclaiming controversies discussed above, as well as the need to re-evaluate the relation between secret intelligence and evidence in terrorism prosecutions, thought should be given to reforming the broad terms of s.38 to list the specific and serious harms that the disclosure of secret information can cause in some cases. A disciplined harm-based approach might help the government avoid overclaiming in the future. It could also address the public suspicion and cynicism that Justice O'Connor accurately noted would follow patently overbroad NSC claims made by the government.

4. Increasing Adversarial Challenge in the Section 38 Process

Another criticism that has been made of s.38 is the ability of the Attorney General to make *ex parte* submissions, and the fact that only the government and the judge can examine the secret information. The Commons committee recommended that either the presiding judge or the party excluded from *ex parte* and *in camera* hearings under s.38 be able to request the appointment of a security-cleared special advocate to challenge the government's case for non-disclosure.⁴²⁷ The Special Senate Committee made a similar recommendation.⁴²⁸ In *R. v. Khawaja*, Chief Justice Lutfy demonstrated some willingness to consider the appointment of a security-cleared special advocate when the Attorney General makes *ex parte* submissions under s.38.11 to support an application for non-disclosure.⁴²⁹ In upholding his decision, however, the Federal Court of Appeal did not indicate that security-cleared special advocates could be appointed under s.38. Indeed, Pelletier J.A. suggested that the court might be powerless to order the disclosure of secret information to anyone in the absence of the agreement of the Attorney General of Canada.⁴³⁰ A security-cleared *amicus curiae* has, however, been appointed to assist with s.38 proceedings in relation to an extradition matter involving allegations of terrorism. One of the conditions of the appointment was that the counsel not have contact with the accused or the accused's lawyer after having seen the secret information without the leave of the Court.⁴³¹ The *amicus curiae* would also not be allowed to see any information covered

⁴²⁷ *Rights, Limits, Security: A Comprehensive Review of the Anti-Terrorism Act and Related Issues* (March 2007) at 81.

⁴²⁸ *Fundamental Justice In Extraordinary Times: The Report of the Senate Committee on the Anti-Terrorism Act* (February, 2007) at 39-42.

⁴²⁹ *R. v. Khawaja* 2007 FC 463

⁴³⁰ *Khawaja v. Attorney General of Canada* 2007 FCA 388 at para 135.

⁴³¹ *Khadr v. The Attorney General of Canada* 2008 FC 46

by informer privilege.⁴³² The same security-cleared lawyer has also been appointed and participated in a 2 day hearing in relation to a second round of s.38 proceedings in the Khawaja trial⁴³³ which will be discussed as a case study later in this section.

The design issues around the use of security-cleared counsel are, as recognized by the Supreme Court in *Charkaoui*, complex and worthy of Parliamentary deliberation. Crucial issues are whether the security-cleared lawyer should be able to consult with the accused or the accused's lawyer after having seen the secret information and whether the security-cleared lawyer can call witnesses or obtain further disclosure. Bill C-3 only contemplates the use of special advocates from a list established by the Minister of Justice with respect to immigration law security certificates, and not under s.38 of the Canada Evidence Act. The judge would have to authorize any communication between the special advocate and other persons about the proceedings after the special advocate has seen the secret information, as well as any attempt by the security-cleared lawyer to obtain further disclosure or call additional witnesses.⁴³⁴ If special advocates find that it is difficult to obtain judicial permission for these activities, their ability to defend the interests of the accused may be seriously attenuated. That said, special advocates might still be in a good position to counter governmental claims for secrecy.

A security-cleared special advocate or *amicus curiae* is not the only option with respect to increasing adversarial challenge. In the Malik and Bagri prosecution, the accused's defence lawyers were able to examine the undisclosed material on an initial undertaking that the information would not be disclosed to their clients. This allowed the lawyers most

⁴³² Ibid at para 37. In *Named Person v. Vancouver Sun* 2007 SCC 43 at para 48, the Supreme Court contemplated that an *amicus curiae* could be appointed to compensate for the non-adversarial nature of proceedings in which both the Attorney General and the informer sought the protection of informer privilege and the accused was excluded. The Court warned, however, that "the mandate of the *amicus* must be precise, and the role of the *amicus* must be limited to this factual task. The legal issues are of another nature. The judge alone makes the legal determination that a confidential informer is present, and that the informer privilege applies. Here, the *amicus* was asked what the scope of the privilege was. Moreover, given the importance of protecting the confidential informer's identity, if a trial judge decides that the assistance of an *amicus* is needed, caution must be taken to ensure that the *amicus* is provided with only that information which is absolutely essential to determining if the privilege applies. Given the mandate of the *amicus* in the present case, it appears that the appointment was inappropriate."

⁴³³ *Canada (Attorney General) v. Khawaja* 2008 FC 560.

⁴³⁴ Bill C-3 *An act to amend the Immigration and Refugee Protection Act* S.C. 2008 c. 3. The special advocate has the ability under s.85.2 (c) to "exercise, with the judge's authorization, any other powers that are necessary to protect the interest of the permanent resident or foreign national." These powers could include making further disclosure requests and the calling of witnesses.

familiar with the case to determine the relevance and usefulness of the information and then to present focused and informed demands for disclosure.⁴³⁵ The alternative under s.38 is that lawyers must make often broad and uninformed demands for disclosure because they have not seen the information. A security-cleared lawyer will require time to become familiar with the case and this will likely cause further delay in s.38 proceedings. At the end of the day, the security-cleared lawyer may never be as familiar with the case as the accused's own lawyer. Although the introduction of adversarial challenge to the Crown's case for non-disclosure has the potential to respond to the dangers of overclaiming of national security confidentiality, it may have more difficulty protecting the accused's right to full answer and defence.

5. Increasing Transparency in the Section 38 Process

Mandatory provisions for closed hearings under s.38.11 were successfully challenged in *Toronto Star v. Canada*.⁴³⁶ Chief Justice Lutfy noted that these mandatory provisions had existed for 25 years, since the introduction of the CEA provisions, but that they could not be justified as a reasonable restriction on freedom of expression and the open court principle. In an earlier case, Chief Justice Lutfy had observed that:

The Federal Court is required by section 38 to keep secret a fact which has been referred publicly in the court or tribunal from which the proceeding emanates... It is unusual that a party to the litigation should be the sole arbiter to authorize the disclosure of information which is or should be public. A court should be seen as having reasonable control over its proceedings in the situation I have just described.⁴³⁷

This passage notes the reality that the Attorney General of Canada could effectively trigger s.38 and its corresponding secrecy provisions. In *Toronto Star v. Canada*, Chief Justice Lutfy held that under the Supreme Court's *Ruby* decision, mandatory closed court provisions could not be justified in those parts of s.38 proceedings that did not consider secret information.⁴³⁸

⁴³⁵ *R. v. Malik and Bagri* 2003 BCSC 1709. See also *R. v. Fisk* (1996) 108 C.C.C.(3d) 63 (B.C.C.A.); *R. v. Guess* (2000) 148 C.C.C.(3d) 321 (B.C.C.A.); *Ontario (Ministry of Correctional Services) v. Goodis* 2006 SCC 31.

⁴³⁶ 2007 FC 128.

⁴³⁷ *Ottawa Citizen v. Canada* 2004 FC 1052 at paras 38, 40.

⁴³⁸ 2007 FC 128 at paras 70-71

The remainder of this section will feature three case studies of the use of s.38 procedures. The first *Kevork* case study involves the use of a predecessor to the present s.38 in a terrorism prosecution in the earlier 1980's. The second *Ribic* case study involves the prosecution of a hostage taking incident in Bosnia in which the use of s.38 in the middle of a criminal trial resulted in a mistrial. This case was influential in producing amendments to s.38 that are designed to ensure that the Attorney General of Canada receives advance warning of s.38 issues. The final case study involves two separate s.38 proceedings including appeals that were taken before the first terrorism prosecution under the 2001 ATA went to trial.

F) Non-Disclosure of CSIS Material Not Seen by the Trial Judge: A Case Study of *R. v. Kevork*

This case study of a terrorism prosecution in the 1980s reveals how the accused may seek disclosure of CSIS material in a terrorism prosecution, how the prosecution can be affected by separate Federal Court non-disclosure proceedings and finally the very difficult position that the criminal trial judge may be placed in when attempting to determine whether non-disclosure of information that they have not seen is consistent with a fair trial.

Between 1982 and 1985, there were three separate acts of terrorism against Turkish targets in Canada. In 1982, a Turkish military attaché, Atilla Altikat, was shot and killed in Ottawa. In 1985, a security guard, Claude Brunelle, was killed in an attack on the Turkish embassy in Ottawa. These cases demonstrate the reality of terrorist violence in Canada before the Air India bombing.

In April, 1982, a Turkish diplomat, Kani Gungor, was shot and left paralysed. Three accused, Haroutine Kevork, Raffic Balian, and Haig Gharakhanian, were charged in March 1984 with conspiracy to commit murder and attempted murder in relation to the shooting. The Crown relied on testimony from two co-conspirators, Hratch Bekredjian and Sarkis Mareshlian, in this prosecution. The accused challenged the credibility of the Crown witnesses, and claimed that they were responsible for the shooting. As with the *Khela* case study, this case study reveals the importance of human sources. There was also an international dimension to the prosecution because the Crown sought to use evidence from electronic surveillance in the United States as well as in Canada. The

case also demonstrates how issues of disclosure, witness protection and secrecy can be closely intertwined in terrorism prosecutions.

The case involved numerous pre-trial motions, both in the provincial superior court and the Federal Court, before the accused pleaded guilty to conspiracy to commit murder. One pre-trial motion involved an attempt by the accused to require the Ottawa police to disclose the identity of a key informant at the bail hearing. Ewaschuk J. noted that the informant would likely have to testify and characterized him as a potential witness. At the same time, however, he concluded that the life of the informant could be in jeopardy if disclosed and that it was not necessary at this preliminary stage to disclose the informant's identity.⁴³⁹ A critical aspect of this ruling was that the credibility of the informant was not relevant to matters to be determined at the bail hearing⁴⁴⁰ or even at the preliminary hearing. Although a preliminary hearing was held in this case, the Crown subsequently used a direct indictment. The subsequent *Stinchcombe* decision on disclosure recognizes that, while evidence and other relevant material should be disclosed to the accused, disclosure is subject to the discretion of the Crown with respect to timing. Crown discretion with respect to the timing of disclosure could allow the government to ensure that witness and source protection measures were in place before a person's identity would have to be disclosed to the accused.

In other pre-trial rulings, Justice Ewaschuk held that evidence derived from American wiretaps could be admitted into the bail hearing without requiring proof of compliance with either Canadian or American constitutional standards. He stressed the informal nature of bail hearings while leaving open the possibility of the Charter applying should such evidence be sought to be admitted at trial.⁴⁴¹ In subsequent cases, the Supreme Court has ruled that the Charter does not apply to the law enforcement actions of foreign officials,⁴⁴² even when they act in co-operation with Canadian officials,⁴⁴³ or to Canadian officials acting abroad.⁴⁴⁴ At the same time, the admissibility of evidence gathered abroad might be found to violate the Charter if it resulted in an unfair trial or another violation of s.7 of the Charter.

⁴³⁹ *R. v. Kevork* [1984] O.J. No. 926

⁴⁴⁰ The accused were denied bail in part because of concerns that they would flee as well as concerns about the safety of the informant if they were released. *R. v. Kevork* [1984] O.J. no. 929.

⁴⁴¹ *R. v. Kevork* (1984) 12 C.C.C.(3d) 339.

⁴⁴² *R. v. Harrer* [1995] 3 S.C.R. 562

⁴⁴³ *R. v. Terry* [1996] 2 S.C.R. 207

⁴⁴⁴ *R. v. Hape* 2007 SCC 26.

During the preliminary inquiry, the accused requested disclosure of electronic surveillance conducted by CSIS, and CSIS profiles with respect to Hratch Bekredjian and Sarkis Mareshlian, the two Crown informants and witnesses, as well as the identity of CSIS officers who conducted physical surveillance on the accused. These issues were relevant in the trial, in part because they might reveal the locations of the Toronto-based accused with respect to a crime that was committed in Ottawa. The preliminary inquiry was adjourned when the Crown objected to the disclosure of such information on grounds of national security confidentiality in Federal Court.

The Attorney General of Canada produced an affidavit in Federal Court proceedings under then s.36.1 and 36.2 of the *Canada Evidence Act* (CEA), from the Director of CSIS, which maintained “that the disclosure would be injurious to national security because it would reveal or tend to reveal the methods used for surveillance, the capacity and ability of the Service to carry out electrical surveillance, the places and means used for same and the identity of the persons involved in conducting it.”⁴⁴⁵ Addy J. denied a request by the accused to cross examine the Director on the affidavit, holding that no cross-examination should be allowed “unless perhaps very weighty and exceptional circumstances are established.”⁴⁴⁶ He noted that there was no explicit right to cross-examine under the CEA procedure, which provided for mandatory *in camera* hearings and a mandatory right by the Crown to make *ex parte* submissions. He stressed the state’s interests in secrecy:

What might appear to the uninitiated, untrained layman to be a rather innocent and unrevealing piece of information might very well, to a trained adversary or a rival intelligence service, prove to be extremely vital when viewed in the light of many other apparently unrelated pieces of information. Because of this and by reason of the extreme sensitivity surrounding security matters it would be a very risky task indeed for a judge to decide whether a certain question should or should not be answered on cross-examination. Furthermore, the person being cross-examined might be put in the difficult position of in fact revealing the answer by objecting to disclosure. Finally, it is easy to foresee that many of the questions in cross-examination would be objected to in

⁴⁴⁵ *Re Kevork* (1984) 17 C.C.C.(3d) 426 at 437 (F.C.T.D.)

⁴⁴⁶ *ibid* at 440

the same manner as the original questions which form the basis of the present application. This would inevitably lead to further inquiries and further applications, thus prolonging the matter indefinitely, creating a real danger of an eventual breach of security.⁴⁴⁷

This conception of the state's interest in security and in particular its emphasis on the mosaic effect, in which one piece of information might provide the enemy with vital clues about ongoing operations, reflected thinking about the state's interest in secrecy at the time. As suggested above, the assumptions behind such understandings of secrecy are not well-suited to terrorism cases.

Addy J. dismissed the accused's request for disclosure of CSIS material without examining the material. He stressed that "the mere fact that Parliament has chosen to allow this court to consider an objection to disclosure on the grounds of national security, national defence or international relations when the subject-matter was previously within the exclusive realm of the executive arm of government, is not any indication that it is in any way less important than before the statutory enactment."⁴⁴⁸

Addy J. upheld the Attorney General of Canada's objection to disclosure of the requested material on national security grounds. He stressed that the proposed line of cross-examination related to the activities of CSIS and to CSIS profiles about the informers. The accused requested the CSIS material primarily to impugn the credibility of the Crown informers but, in Justice Addy's view, the credibility of the informers was already impugned by the admission that they were co-conspirators. He then stated:

...evidence regarding the credibility of a witness is, of its very nature, not the type of evidence which must be considered or taken into account where an objection has been raised pursuant to s. 36.2. Credibility of a witness is not the main issue to be determined even at trial but merely a side issue. It does not go towards directly countering any of the elements of the offence and it is clearly not evidence the production of which is "of critical importance to the defence" (see the Goguen case, *supra*). This test of course applies with equal force

⁴⁴⁷ *ibid* at 439-440.

⁴⁴⁸ *Re Kevork* (1984) 17 C.C.C.(3d) 426 at 431. (F.C.T.D.) See also *Re Gold* [1985] 1 F.C. 642 aff 25 D.L.R.(4th) 285 also not examining the documents.

to evidence sought to be produced at the trial of an accused as well as upon the preliminary hearing. All of the jurisprudence, both Canadian and English, relating to this principle in fact deals with it in the context of an actual trial. One comes to precisely the same conclusion when considering the other purpose for which evidence is sought by the applicants, namely, the theory of the defence that one of the informers had in fact committed the offence of attempted murder. This would not necessarily mean that the three applicants who stand so accused would still not be parties to either the offence of attempted murder or of conspiracy to commit murder. On the above ground alone I would be obliged to hold that the present application must fail.⁴⁴⁹

In upholding the Attorney General's request for non-disclosure, Justice Addy imposed high standards that required the accused to demonstrate at least the probability that the requested material would be helpful to the defence. He concluded that "the applicants are hoping that something might be unearthed which would be helpful. The proposed exercise amounts to nothing less than a fishing expedition or a general discovery. This would be fatal to the application even if the evidence sought to be obtained were of vital importance and had a direct bearing on the issue of guilt or innocence."⁴⁵⁰ Justice Addy's rejection of the accused's disclosure request as "a fishing expedition" that involved the "credibility of the witness", which he characterized as "a side issue" in the criminal trial, stands in stark contrast to Justice Watt's conclusion two years later in *Parmar* that the disclosure of information used to obtain a wiretap warrant was required for full answer and defence and was a "fishing expedition in constitutionally protected waters".⁴⁵¹

Justice Addy also questioned the evidentiary value of the intelligence created by CSIS about the two informers. He stated that the requested CSIS profiles of the Crown witnesses contained "the most glaring type of hearsay and could not be used in evidence even if it had been shown that they probably contained information vital to the defence. The documents could be used neither in examination-in-chief nor in cross-examination of the officers in whose possession they might be. The documents are really general discovery documents which, were it not for the subject-matter,

⁴⁴⁹ Ibid at 434

⁴⁵⁰ Ibid at 435

⁴⁵¹ *R. v. Parmar* (1986) 34 C.C.C.(3d) 260 at 279-280 (Ont.H.C.) discussed infra Part III.

might possibly be compellable in an examination for discovery in a civil suit but their production could never be compelled at trial in any type of action governed by the rules of evidence."⁴⁵² Today, *Stinchcombe* disclosure obligations apply to much information that would not necessarily be admissible at trial, and the Supreme Court has recognized that the accused's right to full answer and defence can be violated by denying the accused information that could open up valuable lines of inquiry.⁴⁵³ That said, any inability of the accused to use intelligence at trial would be a factor to be considered in determining the effect of non-disclosure of intelligence on the accused's right to full answer and defence.

After the request for non-disclosure under the CEA was decided in favour of the Attorney General of Canada, the preliminary inquiry resumed. After hearing 30 days of evidence, the provincial court judge committed the accused on the conspiracy to murder charges, but not on the attempted murder charges. The Crown subsequently issued a direct indictment on the attempted murder charges and this procedure became the subject of an unsuccessful Charter challenge by the accused. The direct indictment procedure was held not to violate the Charter. The Court of Appeal subsequently held that it had no jurisdiction under the Criminal Code to hear an appeal of this determination. It noted in this regard that there were "strong policy reasons against interrupting the trial process with appeals to the Court of Appeal. The same policy reasons in our view apply to the delay of criminal trials by proceedings of this sort. The fragmentation of criminal proceedings should not be encouraged."⁴⁵⁴ The Court also rejected an attempt to make an interlocutory civil appeal, holding that the proper pleadings and notice to the Attorney General had not been made by the accused.⁴⁵⁵ Similar pre-trial appeals are available under both ss. 37 and 38 of the CEA and, as will be seen in connection to the ongoing Khawaja case, they can delay terrorism prosecutions.

The accused in the *Keveork* case renewed their Charter challenge to the direct indictment procedure before the criminal trial judge, but this was rejected on the basis that "the accused had no occasion to complain. They were already in custody on the conspiracy to murder charge; they were held without bail on that charge. They had the benefit of extremely thorough and complete discovery; the process of discovery remains an

⁴⁵² *Re Keveork* (1984) 17 C.C.C.(3d) 426 at 431 at 435 (F.C.T.D.).

⁴⁵³ *R. v. Taillifer* [2003] 3 S.C.R. 307.

⁴⁵⁴ *Re Keveork* (1985) 21 C.C.C.(3d) 369 at 372 (Ont.C.A.).

⁴⁵⁵ *ibid* at 373

on-going one, as I am advised. The discharge on the attempted murder count was at least open to question..."⁴⁵⁶

The trial judge considered the non-disclosure order made by Justice Addy under the *Canada Evidence Act* in another pre-trial motion. Smith J. noted that the conflicts between the state's interests in secrecy and the accused's rights were complex and confronted in many democracies. "The question, simply put, is whether the accused can, on the facts of this case, make full answer and defence in the absence of the disclosure which was denied them. This calls for a definition of the scope of the right to make full answer and defence. Is it absolute? If not, what are the parameters of this right, assuming a violation of the right at common law or under statute law or of the constitutional right to make full answer and defence? Can resort be had to s. 1 of the Charter in order to give primacy to national security and compel the accused to stand trial without access to the information sought?"⁴⁵⁷

The accused again sought to obtain evidence of any CSIS wiretaps and CSIS surveillance before the trial judge. This illustrates how a pre-trial determination by the Federal Court may not end continuing attempts to obtain disclosure from the trial judge. The judge noted that the accused "argued that the electronic surveillance which is the subject of a subpoena, if it does exist for its very existence is not admitted, will nail the coffin shut and destroy completely the co-conspirators' credibility. The case is far too complex, in my view, to enable me to accept this extreme contention. The most that can be said at this stage is that it might well prove material and relevant one way or the other on the issue of the reliability of the evidence of the co-conspirators. I should again emphasize that it is clear that, their credibility has already been quite significantly impaired at the preliminary hearing."⁴⁵⁸ This suggests that the precise effects of non-disclosure can only be evaluated in relation to the precise issues in the case and the totality of the evidence presented at trial. The Federal Court judge presiding at a pre-trial hearing would not be in the same position as the trial judge in determining how non-disclosure would relate to the live issues in the trial. The trial judge expressed unease with the fact that Justice Addy had not examined the material that he ordered not to be disclosed. He stated:

⁴⁵⁶ *R. v. Kevork* (1985) 27 C.C.C.(3d) 271 at 281

⁴⁵⁷ *R. v. Kevork* (1985) 27 C.C.C.(3d) 523 at 526.

⁴⁵⁸ *R. v. Kevork* (1985) 27 C.C.C.(3d) 523 at 530

I am, nevertheless, prepared to accept, as I read his reasons, that in Justice Addy's mind concerns for national security occupied a priority position when compared with the rights of the accused. In the end though, as already stated, he was only concerned with disclosure. He did not choose to inspect the material. I feel uncomfortable with the notion of lack of inspection in Federal Court. If the Chief Justice or his judge designate should, in any given case, be satisfied not to order disclosure in the interests of national security without having inspected, the trial judge may well be on the horn of a real dilemma if, in his judgment, inspection is needed.⁴⁵⁹

As will be seen in subsequent cases, the Federal Court has moved away from its early position that, generally, judges need not inspect material when deciding matters of national security confidentiality. This at least ensures that a judge, albeit not the trial judge, examines the material over which the Attorney General of Canada seeks non-disclosure.

Smith J. commented at length on the implications of the two-court approach which took issues of national security confidentiality away from the trial judge and placed them in the hands of specially designated judges of the Federal Court. He stated:

Parliament has reserved the matter of possible injury to international relations, national defence or security to the Chief Justice of the Federal Court or to his justice designate with certain directions affecting the balancing process as between competing interests. There is now in this country a bifurcation of duties which admittedly did not exist at common law. It must now be accepted by trial judges that the privilege in those three areas of defence, international relations and national security, to the extent that they were committed to the judiciary by statute, have no place in the trial courtrooms in so far as disclosure or discovery is concerned. But at the same time trial courts cannot say that by way of corollary they must abdicate the responsibility of ensuring that persons accused of crimes are given a fair trial and afforded the right to make full answer and defence and are allowed

⁴⁵⁹ *ibid* at 536.

to otherwise enjoy all of the rights and privileges traditionally reserved to them, in what, as we now have, a constitutionally entrenched form. Disclosure will not be available but s. 24(1) will enable courts to fashion a remedy, where one is indicated, in the appropriate case.⁴⁶⁰

The trial judge accepted that Parliament had allocated questions of national security confidentiality to the Federal Court, but he also concluded that questions of full answer and defence, fair trial, and Charter remedies that could arise as a consequence of non-disclosure orders made by the Federal Court would be decided by the trial judge. Justice Smith's focus on preserving a fair trial has been confirmed in s.38.14 of the CEA, which affirms the trial judge's right to make any order necessary to protect the accused's right to a fair trial while, at the same time, requiring the trial judge to comply with non-disclosure orders made by the Federal Court.

The trial judge appeared to have misgivings about the two-court structure of the CEA. He noted that: "Blame must be laid squarely at the feet of Parliament which unwittingly may well have created an impasse in certain cases by resorting to two courts instead of one and assigning tasks to each of them that collide or run at cross-purposes to one another." He added that "there appears to be nothing left to do at trial except to consider the impact of the Federal Court determination on the exigencies of a fair trial...Parliament could not have intended to give the Federal Court jurisdiction nor, in my opinion, could such jurisdiction be exercised by the Federal Court in such a way as to operate in derogation of the duty imposed on trial judges, as courts of competent jurisdiction, to enforce the rights of the accused in the course of the trial, rights that are now constitutionally entrenched."⁴⁶¹ These comments raise the possibility that, as a result of the two-court approach, trial judges may err on the side of protecting the accused's right to a fair trial by staying proceedings: because they are deprived of the ability to see the evidence that the accused wants disclosed or because the trial judge is unable to balance between the competing interests in secrecy and disclosure.

Justice Smith rejected the argument that all evidence must be disclosed to the accused if a prosecution was to occur. He stated:

⁴⁶⁰ *ibid* at 537.

⁴⁶¹ *ibid* at 538, 540.

In the context of national security, I reject the contention that the moment there is found to be some material evidence in possession of the State to which access is denied, the State must adopt the “stark choice rule” in *U.S. v. Reynolds et al.* (1953), 345 U.S. 1, and desist from prosecution. I allow, however, that this begs the very thorny question of inspection. The defence urges that I not adopt the “novel” notion that evidence must be essential and critical before a stay will be granted. The contention is that in the criminal field a government could only invoke an evidentiary privilege at the price of letting the defendants free as long as there was material evidence being withheld (the stark choice rule). I am not convinced that that has been the case at common law or in the U.S. I have already referred to the Classified Information Procedures Act in the U.S. The court, under that Act, is authorized to delete certain portions of the classified material. The proceeding which is contemplated is separate from the trial and is *ex parte*. The government may even substitute a summary.⁴⁶²

The trial judge was attracted to a flexible approach to reconciling competing interests in fairness and secrecy. He accepted that a stay was not the only possible remedy and other remedies could include a requirement that a witness be prevented from testifying unless disclosure was made, or that the witness testify without revealing his identity or testify by means of written questions and answers that could be screened for secrets. At the same time, he indicated that “most of these remedies” would not be available to the trial judge because they would have the effect of collaterally attacking the Federal Court order that the CSIS material not be disclosed to the accused. In other words, the Federal Court, rather than the trial judge, would have to impose conditions on disclosure such as the use of summaries or substitutions. Again, this approach has now been codified in s.38.06(2) of the CEA.

The trial judge was left in the difficult position of not being able to alter the Federal Court’s non-disclosure order and of having a limited range of practical remedies that could be applied at trial. Smith J. recognized that a judicial stay of proceedings was a drastic remedy that would

⁴⁶² *ibid* at 543

permanently stop the prosecution. He indicated that a stay would only be an appropriate remedy if the evidence not disclosed “is critical or essential...without which the applicants will probably not be able to make full answer and defence”. He elaborated:

Such a burden imposed upon accused persons to show that the evidence is crucial or essential is, in my view reasonable if we are to avoid fishing expeditions in all cases when it is likely that CSIS had some hand in gathering information. CSIS will be involved in virtually all cases where the security of the State and of its citizens is in jeopardy through acts precisely of the kind that will be under investigation in this trial.⁴⁶³

Applying this test, the trial judge concluded that a stay was not appropriate because the accused had not established that it was denied evidence essential to a fair trial or full answer and defence by being denied access to CSIS wiretaps, CSIS surveillance or CSIS profiles. He concluded:

To stay in the case at hand, or in any case, where only some or any material information is withheld comes close to conferring immunity from prosecution upon all those charged with terrorist acts. The defence position, in my view, had no support at common law and the Charter does not require that it be adopted...., neither credibility of the co-conspirators, nor the alleged alibi, nor the evidence relating to the weapons, nor the American wiretaps which may not even be admissible and as to which I have no real present knowledge, nor a combination of all make a compelling case, in my judgment, for this court to intervene to prevent a Charter violation at this stage.⁴⁶⁴

Even while reaching this conclusion that a stay was not required and the accused had not established a violation of the right to full answer and defence, the trial judge expressed misgivings, namely that “the absence of inspection does bother me. A case could arise where the defence will make a strong case for disclosure, for purposes of a fair trial, in which the Federal Court refused even to inspect. The trial court might then have to

⁴⁶³ *ibid* at 546

⁴⁶⁴ *ibid* at 546

impose a conditional stay urging inspection at least so that an informed decision can be made.”⁴⁶⁵ This statement held open the possibility that a conditional stay by a trial judge could require the Attorney General, and perhaps the Federal Court, to reconsider a non-disclosure order. A conditional stay might provide time to make provision for the security of vulnerable informers or for an ongoing operation, or to obtain an amendment of a caveat that restricted the use of information obtained from a foreign agency.

The trial in the *Kevork* case involved many pre-trial motions, including testimony about an FBI wiretap and testimony from the victim before the jury.⁴⁶⁶ In late April, 1986 the trial was aborted when the accused agreed with the Crown’s offer to plead guilty to the conspiracy charge in exchange for dropping the attempted murder charge. Although it is impossible to know for sure, the undisclosed CSIS material might have been more relevant to the attempted murder charge if it disclosed the whereabouts of the Toronto accused on the days in question.

Kevork was sentenced to nine years imprisonment, Balian was sentenced to six years imprisonment and the youngest accused, Gharakhanian was sentenced to two years less a day. The Crown appealed the sentences and the Court of Appeal increased Balian’s sentence to eight years imprisonment. It, however, rejected the Crown’s appeal of Kevork’s sentence on the basis that when double time was counted for pre-trial custody it was only six months less than the fourteen years maximum. The Court of Appeal also took note that Kevork’s decision to plead guilty had avoided a long trial. The Court of Appeal also rejected the Crown’s appeal of Gharakhanian’s sentence in part on the grounds that he was only seventeen years old.⁴⁶⁷ Kevork was subsequently found guilty of perjury in relation to material submitted at sentencing and received an additional year of imprisonment.⁴⁶⁸

The *Kevork* prosecution reveals how accused in terrorism prosecutions may request access to intelligence generated by CSIS and other intelligence agencies. Today the proceedings would be conducted differently in some

⁴⁶⁵ *ibid* at 546

⁴⁶⁶ 135 potential jurors were rejected after being questioned about whether they could fairly try a case involving an allegation of terrorism and in light of the pre-trial publicity in the case. Special security arrangements were also made for the trial. John Kessel “Jury selection finished for envoy’s shooting trial” *Ottawa Citizen* March 21, 1986 C.1.

⁴⁶⁷ *R. v. Kevork* (1988) 29 O.A.C. 387.

⁴⁶⁸ John Kessel “Chronology of terror: the plot to kill a Turkish diplomat” *Ottawa Citizen* June 14, 1986 A1; “Convicted in envoy plot, Armenian’s term extended” *Globe and Mail* Jan 18, 1988 A15.

respects. The Federal Court would almost surely examine the information that was the subject of the non-disclosure application. At the same time, however, the main problems revealed by the Kevork case study--namely the need for separate proceedings in the Federal Court and the dilemma of trial judges having to decide whether a fair trial was possible in light of a non-disclosure of material that the trial judge had not seen--would remain. In addition, the case today would have to be decided in light of more generous understandings of both 1) the accused's right to disclosure of all relevant and non-privileged information; and 2) the accused's right to full answer and defence, which could be infringed by the cumulative effects of non-disclosure, including non-disclosure of information that might open up important avenues of investigation and adversarial challenge to the accused.

G) Use of Section 38 During a Criminal Trial: A Case Study of *R. v. Ribic*

Nicholas Ribic was charged with four counts of hostage-taking, under s.279.1 of the Criminal Code, in relation to events in Bosnia involving the Canadian Armed Forces. The case involved the infamous chaining of a Canadian soldier, Captain Patrick Rechner, to a pole in an effort to stop NATO bombing of Serb forces in May, 1995. This case is particularly interesting because it involves litigation both before and after the major amendments made to s.38 of the *Canada Evidence Act* under the 2001 *Anti-Terrorism Act*. It involves two criminal trials, one which failed to reach verdict because of the surprise, delay and fragmentation of the trial caused by s.38 proceedings, and another trial that successfully reached a verdict despite litigation and appeal of national security confidentiality issues before the Federal Court under s.38.

Ribic consented to his extradition from Germany in 1999, and he was arrested and released on bail upon his return to Canada. The trial was held in Ottawa despite the fact that Ribic lived in Edmonton.⁴⁶⁹ The Criminal Code now provides for the possibility of terrorism cases to be tried outside the territorial jurisdiction in which they were alleged to have been committed.⁴⁷⁰ A preliminary inquiry was not completed and, in October, 2000, a direct indictment was preferred, with a trial being scheduled for November, 2001. Because of various disclosure and pre-trial motions, including motions before the Federal Court under s.38, this trial

⁴⁶⁹ For an order for extra costs caused by this choice of venue see *R. v. Ribic* [2000] O.J. no. 565.

⁴⁷⁰ Criminal Code s.83.25.

was postponed until October, 2002. At that time, the Crown presented its case to the jury over eight days and by calling six witnesses. After the Crown's case went in, Ribic's lawyers announced that they proposed to call two witnesses with the Canadian military who had been in Bosnia and who they said had extensive information about the hostage-taking incident.

The issue of whether the proposed witness's evidence could be given was litigated in the Federal Court under s.38 of the *Canada Evidence Act*. In December, 2002, the trial judge recalled the jury and explained that "this is an unfortunate situation over which I, and frankly counsel, have no control", and asked the jury if they were willing to return in January. The jury agreed to the postponement.⁴⁷¹ The trial judge, however, concluded on January 20, 2003, that with more Federal Court proceedings pending, he must dismiss the jury and declare a mistrial.⁴⁷² This incident reveals how a bifurcated court process for determining national security confidentiality can adversely affect the criminal trial process, to the point of preventing the court from reaching a verdict. If similar issues had arisen during the Malik and Bagri trial, and if the accused had not re-elected to be tried by judge alone, there would also have been a risk of a mistrial.

1. Federal Court Pre-Trial Proceedings Over Disclosure

A significant part of the delay that led to a mistrial being declared in the Ribic case in 2003 was related to the fact that there was no advance notice by the defence of the s.38 issues until a jury had been empanelled. Section 38.01(1) as amended by the *Anti-Terrorism Act* is now designed to place an obligation on all parties to notify the Attorney General of s.38 issues "as soon as possible." This could potentially prevent the problems that arose in Ribic's first trial. The accused could have given early notice of the intent to call the witnesses; or the witnesses themselves, if contacted by the accused, might have notified the Attorney General or the person presiding at the hearing, as contemplated under s.38.01(3) or (4).

Although the new provisions can be helpful, there is no explicit sanction for a failure to give advance notice. A trial judge might have difficulty justifying denying the accused an opportunity to call perhaps important evidence in full answer and defence as a sanction for late notice. The

⁴⁷¹ "Ribic's hostage-taking trial to proceed" Edmonton Journal Dec. 10, 2002 p.A10.

⁴⁷² This account is taken from *R. v. Ribic* [2004] O.J. No. 2525 in which Rutherford J. rejected an application for a stay of proceedings on the basis of a violation of the s.11(b) Charter right to a trial in a reasonable time.

accused could argue that the case to meet principle⁴⁷³ also justifies some delay in informing the Attorney General of what witnesses should be called. In other words, the Ribic scenario in which s.38 issues have to be litigated in the middle of a criminal trial could still arise.

The first Ribic trial involved a range of pre-trial motions being heard by the Federal Court in relation to various disclosure matters. In all of these cases, the Federal Court judge examined the information over which non-disclosure was sought. In March, 2002, Hugessen J. of the Federal Court, after hearing from both parties, including *ex parte* representations from CSIS, decided that he would examine the material that was the subject of a non-disclosure claim. In reaching this decision, he noted that the criminal trial judge in the Ontario Superior Court had indicated in a judgment that it would be helpful to see the withheld material. Hugessen J. commented: "While that view does not, of course, bind me, I think it is entitled to the very greatest respect for it comes from the person who will ultimately have to make the decision as to the admissibility and relevance of the evidence at trial."⁴⁷⁴ This statement demonstrates how the Federal Court judge can be aware of, but not bound by, the judgments of the trial judge about whether material should be disclosed. The ultimate decision about what the trial judge could see, however, would be determined by the Federal Court after it had balanced the competing public interests in disclosure and non-disclosure.⁴⁷⁵

Hugessen J. ordered that some CSIS documents be disclosed to the accused, but that they be subject to editing. In the course of this editing, he "excluded information regarding sources, names of agents of the Service, routing information, codes and things of that technical nature which are in fact of no interest to the defence at all."⁴⁷⁶ He also excluded "information which would be likely to reveal investigative techniques again of no interest to the accused and all references to authorizations sought or obtained under the Canadian Security Intelligence Service Act". Finally, he excluded "information which would be likely to affect Canada's international relations" and which "was of no conceivable interest or help to the accused in the conduct of his defence."⁴⁷⁷ The editing used in this

⁴⁷³ *R. v. Rose* [1998] 3 S.C.R. 262.

⁴⁷⁴ *Ribic v. Canada* [2002] F.C.J. no 384 at para 4.

⁴⁷⁵ As Hugessen J. stated "Whether or not the withheld material should be disclosed is, of course, another matter and will depend upon the balancing of the competing interests involved, a process which I now propose to undertake." *Ibid* at para 6.

⁴⁷⁶ *Ibid* at para 7.

⁴⁷⁷ *Ibid* at paras 9- 10

case represents an attempt to protect the legitimate objects of national security confidentiality while, at the same time, disclosing to the accused evidence that is relevant to the criminal trial.

Hugessen J. deleted information subsequent to the event in question on the basis that it had “no direct bearing on the matters charged against the applicant”.⁴⁷⁸ Sometimes the precise and discrete nature of the criminal charge will make it easier to rule that matters subject to national security confidentiality are not relevant. At the same time, criminal charges in terrorism cases, particularly those relating to conspiracies, facilitation or participation in a terrorist group, may be so wide-ranging that more material in the state’s possession will be relevant to the charge.

Hugessen J. deleted from the disclosed material “analyses conducted by the Service of the information which is essentially of a forward looking nature taking the form of prediction of what may be going to happen...”⁴⁷⁹ Intelligence about possible future security threats, matters that lie at the heart of the security intelligence mandate, may often not be valuable to the defence. In some contexts, the distinctions between predictive and even speculative intelligence and concrete evidence may be so great that the accused may not have a legitimate interest in access to the intelligence in order to defend him or herself in court. In other contexts, however, the information as it relates to informers or alibi witnesses may be more closely related to the accused’s right of full answer and defence.

Another pre-trial proceeding was held over whether the accused could have access to five documents held by the Department of National Defence (DND) that did not make any reference to Mr. Ribic. Lutfy A.C.J. held that most of the DND documents should not be disclosed, either because they were not relevant to the case or marginally relevant. He ordered the disclosure of one document that related to hostages on the basis that it was not “clearly irrelevant”, as that standard is understood in *Stinchcombe* and that it was also “‘likely relevant’ to the ability of the respondent Ribic to make full answer and defence.”⁴⁸⁰ Lutfy A.C.J. also stressed that the criminal context of the case affected the balancing test to be applied under s.38.06(2) when he stated:

⁴⁷⁸ *ibid* at para 10.

⁴⁷⁹ *ibid* at para 7.

⁴⁸⁰ *R. v. Ribic* [2002] F.C.J. no. 1186 at para 19

Decisions in other section 38 applications where documents were not inspected or which came to this Court from a commission of inquiry, an administrative tribunal or a civil action can be distinguished from this case.

The respondent Ribic is accused with hostage taking under section 279.1 of the Criminal Code in the Ontario Superior Court of Justice and, if convicted, is liable to imprisonment for life. The seriousness of the criminal charges caused my inspection of the documents without applying the two-step procedure in *Goguen*... Parliament has required the designated judge to balance competing interests, not simply to protect the important and legitimate interests of the state.

In weighing the competing interests, the designated judge is assisted, it seems to me, by specific evidence concerning the harm caused in the disclosure of an expurgated document for a criminal trial involving serious charges.⁴⁸¹

The accused in this case recognized some legitimate national security interests and did not seek “the names of sources or targets, addresses, routing information, codes or encryptions, file numbers, sources of information, whether they be individuals or otherwise, or information concerning the technical means or other methods of information gathering.”⁴⁸² In other contexts, however, an accused could argue that the source of information, whether individual or institutional, was relevant to its reliability and that the method of information gathering was relevant to the legal admissibility of the information.

A month later, Hugessen J. decided another pre-trial motion involving the disclosure of material relating to the time and location of the alleged crime which was held by DND but obtained from a foreign government under a promise of non-disclosure. He recognized that, taken by itself, this case raised what some have called “a clash of the titans”: the accused’s right to full answer and defence against the state’s interest in national security, national defence and international relations. In the end, however, he decided that the material could be disclosed because the foreign

⁴⁸¹ *ibid* at paras 17-18, 22-23.

⁴⁸² *Ibid* at para 9

government had not responded to repeated requests by Canada to allow the disclosure of the document. He drew an adverse inference that the matter was “clearly not a matter of prime importance”⁴⁸³ to the foreign power, and ordered that the material be disclosed with some information edited out. This ruling is significant because it demonstrates that caveats or restrictions on the use of intelligence are not absolute and can be subject to requests for amendments when necessary to satisfy disclosure obligations. It is consistent with the modifications of the third party rule discussed above.⁴⁸⁴

2. The Proceedings in Relation to the Witnesses that Ribic Proposed to Call at Trial

A number of s.38 motions were heard in the Federal Court after the Crown had put in its case to a jury in the Ontario Superior Court, but before a mistrial was declared. These motions dealt with the difficulties presented by attempts by the accused to call witnesses to testify about secret information. In early January, 2003, Blanchard J. of the Federal Court decided a number of issues under s.38 of the *Canada Evidence Act*, including the admissibility of a transcript of testimony of the two witnesses from the military that the accused had proposed to call at the criminal trial about the events in Bosnia, but who were subject to the s.38 notice. Chief Justice Lutfy had in November, 2002, ordered that the two witnesses be asked questions by a security-cleared lawyer employed by the Attorney General of Canada. The questions were, however, submitted by the accused’s lawyer. The accused challenged this innovative procedure as violating his right to fully cross-examine witnesses and to put relevant witnesses before the trier of fact in the criminal trial, and thus, his right to full answer and defence, but these arguments were rejected by Blanchard J. and subsequently by the Federal Court of Appeal. They stressed that the novel procedure was used when issues of national security confidentiality arose in the middle of the criminal jury trial and when there was no time for the accused’s lawyers to seek security clearances. Letourneau J.A. explained for the Court of Appeal that “the jury was kept waiting. The applicable legislation was new and a solution had to be found quickly.... Creativity often carries their proponents into the realm of the unusual, as it did here, but I am satisfied that fairness accompanied them throughout their journey.”⁴⁸⁵

⁴⁸³ *R. v. Ribic* [2002] F.C.J. no. 1835 at para 8.

⁴⁸⁴ *Attorney General of Canada v. Khawja* 2007 F.C. 490.

⁴⁸⁵ *R. v. Ribic* [2003] F.C.J. no 1964 at paras 43, 56 (Fed.C.A.).

Both Blanchard J. and Letourneau J.A. expressed concerns that it was neither safe nor practical to allow the two witnesses to give *viva voce* evidence in the criminal trial. In a passage that was specifically endorsed by the Court of Appeal, Blanchard J. warned of the danger that testimony at a criminal trial might inadvertently reveal secret and damaging information:

In their testimony, the two witnesses wove innocuous information with information that cannot be publicly disclosed. There is no demarcation line easily separating what is authorized from what is not. Implementing a demarcation line, in the context of a criminal trial conducted before a jury, is clearly not practical if not impossible. The learned trial judge will not have the benefit of reviewing all of the information to allow him to fully appreciate the potential impact of a disclosure of what may appear to be an innocuous piece of information. What may appear to be trivial information may in fact be the one missing piece in the jigsaw piece created by a hostile agency.⁴⁸⁶

The reference to the jigsaw puzzle may reflect what has been described as the mosaic effect in terms of the dangers of releasing information.⁴⁸⁷ The Ribic case involved military action and alliances. As suggested above, concerns about revealing evidence to the enemy through the mosaic effect may be less pressing with respect to non-state actors in loosely organized terrorist cells.

Leaving the applicability of the mosaic effect to counter-terrorism investigations aside, the above comments by Blanchard J. are significant because they reveal some of the difficulties created by s.38's two-court structure. The Federal Court, which had heard *ex parte* submissions from various witnesses about the harms of disclosing the material,⁴⁸⁸ was concerned the criminal trial court might not have the full picture about possible harms to security. At the same time, however, it could also be argued that the Federal Court itself might not be in the best position to

⁴⁸⁶ *R. v. Ribic* [2003] F.C.J. no. 1965 at para 35 per Blanchard J. and endorsed in *R. v. Ribic* [2003] F.C.J. no. 1964 at para 51 (Fed.C.A.).

⁴⁸⁷ See for example *Henrie v. Canada (Security Intelligence Review Committee)* (1988) 53 D.L.R.(4th) 568 affd (1992) 88 D.L.R.(4th) 575 (Fed.C.A.).

⁴⁸⁸ During a five day hearing, Blanchard J. had heard *in camera* and *ex parte* testimony from three witnesses: "a member of the Directorate General Intelligence Division of the Canadian Forces, an employee of another governmental agency; and a representative from the Department of Foreign Affairs and International Trade." *R. v. Ribic* [2003] F.C.J. no. 1965 at para 7.

have the full and evolving picture about the importance of the information to the accused. These comments underline the difficulties of a bifurcated process in which issues of national security confidentiality are decided by one judge in the Federal Court who has heard *in camera* evidence from government witnesses about the harms to national security, national defence or international relations while a criminal trial judge must decide the effect of any non-disclosure order on the accused's right to a fair trial.

Although the bifurcated process has significant shortcomings, both in terms of efficiency and in terms of giving the relevant decision-makers the fullest information on which to make their decisions, the Court of Appeal in *Ribic* found that it had one benefit to the accused: namely it provided a means through which the accused could disclose his defence to the Federal Court to assist in its decision-making, but without disclosing it to the separate prosecutorial team or to the judge who would decide the criminal charges in the Superior Court. Letourneau J.A. stated that "the whole process leading to the determination of the State secrecy privilege compels an accused to reveal his defence and disclose information that supports the defence."⁴⁸⁹ Nevertheless:

It is of fundamental importance to note that disclosure of the sensitive information that the appellant [the accused] wants to rely upon is not made to the prosecution, but, under the seal of absolute confidentiality, to the Attorney General and a designated judicial forum where the matter will be decided in private. It is therefore not a disclosure which violates an accused's right to silence and the presumption of innocence in criminal proceedings. In addition, as the appellant requests in the present instance, this Court has the authority to issue an order that none of the information disclosed in the context of the section 38 process be released without the consent of the defence. In my view, sufficient and adequate guarantees are offered by the system, which protect an accused's right not to disclose to the prosecution his defence.⁴⁹⁰

Similarly, the criminal trial judge also stressed that the prosecutors in the criminal case, although "employed and instructed federally", took no

⁴⁸⁹ *R. v. Ribic* [2003] F.C.J. no 1964 at para 29 (Fed.C.A.).

⁴⁹⁰ *ibid* at para 30.

part in the Federal Court proceedings and “were not privy to any of the information”⁴⁹¹ in those proceedings. Section 38.11(2) allows the accused to make *ex parte* representations before the Federal Court judge.

In addition to the above procedural innovations, the decisions by Blanchard J. and the Federal Court of Appeal are also interesting because of their reconciliation of competing interests in security and disclosure. Much of the material held by DND was obtained from NATO in the expectation that it would not be disclosed. There were concerns that disclosure would prejudice future intelligence sharing from allies as well as operations. Blanchard J. determined that much of the information, for example that relating to operations not related to the hostage-taking incident, was simply not relevant and need not be disclosed.⁴⁹² Other information was relevant and “logically probative to issues that may be raised at trial and certainly could assist the jury in putting the events leading up to the hostage-taking and the event itself into the proper context.”⁴⁹³ Nevertheless, he determined that there was enough material in the edited transcripts to inform the jury about the relevant context of events leading up to the hostage-taking.⁴⁹⁴ This decision, which was upheld by the Court of Appeal, demonstrates a willingness to allow evidence that has been edited to reconcile the competing demands for secrecy and disclosure. At the same time, decisions by the Federal Court that material is not relevant under *Stinchcombe* may be handicapped by the fact that all the circumstances that might arise from the trial, including those that could arise from the accused’s defence, may not be known to the Federal Court judge who is not the trial judge or generally charged with reviewing matters of the adequacy of the Crown’s disclosure in criminal cases.

3. The Federal Court of Appeal’s Three Step Approach

The Court of Appeal rejected the accused’s request to disclose all relevant evidence, subject to the Attorney General issuing a certificate under s.38.13

491 *R. v. Ribic* [2004] O.J. no. 2525

492 *R. v. Ribic* [2003] F.C.J. no. 1965 at para 25.

493 *Ibid* at para 26

494 Blanchard J. concluded that the undisclosed “information, although corroborative, would not, in my view, disclose any new information that would be helpful to the defence that is not already contained in the expurgated transcripts of the testimony of the two witnesses....for the purposes of the defences to be raised at trial, the expurgated transcripts fairly reflect the nature and substance of the testimony of the two witnesses. I therefore conclude that the information which I include in this second category, although relevant, need not be disclosed.” *Ibid* at para 37

that would block the court ordered disclosure on the basis that “the Federal Court would be remiss of its duties under the act if it were to endorse the appellant’s philosophy of general disclosure based on mere relevancy, a philosophy that can only lead to and incite fishing expeditions.”⁴⁹⁵ At the same time, the Court of Appeal recognized that accused will often have to make broad initial claims for disclosure because they have not seen the information that the government seeks to protect.⁴⁹⁶ In addition, the idea that disclosure on the basis of “mere relevancy...can only lead to and incite fishing expeditions” is in some tension with the idea in *Stinchcombe* that disclosure of all relevant evidence held by the Crown is required to respect the accused’s Charter rights and prevent miscarriages of justice. This decision raises questions whether the Federal Court might apply a more restrictive approach to *Stinchcombe* than criminal courts.

The first step in applying s.38 is to determine whether the evidence is subject to *Stinchcombe* disclosure requirements as relevant information, either exculpatory or inculpatory, that would be useful to the defence. The accused will bear the onus of demonstrating relevance and the court should usually examine the information to determine whether it is relevant. This represents an important and salutary departure from earlier precedents, in which the Federal Court had ordered non-disclosure without even examining the information. The Court of Appeal commented that the relevance standard is “undoubtedly a low threshold”.

⁴⁹⁷ Nevertheless, the relevance standard was used in *Ribic* to decide that most of the five hundred and fifty-five pages of transcript were not relevant and not subject to disclosure.⁴⁹⁸ The differences between the mandate of police forces and security intelligence agencies may very well result in a significant amount of background intelligence not being relevant to a criminal charge. At the same time, however, broad-based criminal charges, whether based on conspiracies or on new terrorism offences such as participation in a terrorist group, may make the activities of the accused and a broad range of associates relevant over a long period of time.

If the information is determined to be relevant, the second step is to determine whether the executive has established that the disclosure of the information would be injurious to international relations, national defence or national security. Letourneau J.A. indicated that the Attorney’s

⁴⁹⁵ *R. v. Ribic*[2003] F.C.J. no 1964 at para 13.

⁴⁹⁶ *Ibid* at para 11

⁴⁹⁷ *Ibid* at para 17

⁴⁹⁸ *ibid* at para 40-41

General submission as to the injury of disclosure “should be given considerable weight” because “of his access to special information and expertise”.⁴⁹⁹ Letourneau J.A. elaborated the deferential standard to be used in determining whether the disclosure of the information would be injurious to international relations, national defence or national security:

The judge must consider the submissions of the parties and their supporting evidence. He must be satisfied that executive opinions as to potential injury have a factual basis which has been established by evidence: *Home Secretary v. Rehman*, [2001] 3 WLR 877, at page 895 (HL(E)). It is a given that it is not the role of the judge to second-guess or substitute his opinion for that of the executive. As Lord Hoffmann said in *Rehman, supra*, at page 897 in relation to the September 11 events in New York and Washington, referred to in *Suresh v. Canada (Minister of Citizenship and Immigration)*, [2002] 1 S.C.R. 3, at paragraph 33:

They are a reminder that in matters of national security, the cost of failure can be high. This seems to me to underline the need for the judicial arm of government to respect the decisions of ministers of the Crown on the question of whether support for terrorist activities in a foreign country constitutes a threat to national security. It is not only that the executive has access to special information and expertise in these matters. It is also that such decisions, with serious potential results for the community, require a legitimacy which can be conferred only by entrusting them to persons responsible to the community through the democratic process. If the people are to accept the consequences of such decisions, they must be made by persons whom the people have elected and whom they can remove.

This means that the Attorney General’s submissions regarding his assessment of the injury to national security, national defence or international relations, because of his access to special information and

⁴⁹⁹ *ibid* at para 19

expertise, should be given considerable weight by the judge required to determine, pursuant to subsection 38.06(1), whether disclosure of the information would cause the alleged and feared injury. The Attorney General assumes a protective role *vis-à-vis* the security and safety of the public. If his assessment of the injury is reasonable, the judge should accept it. I should add that a similar norm of reasonableness has been adopted by the House of Lords: see *Rehman*, *supra*, at page 895 where Lord Hoffmann mentions that the Special Immigration Appeals Commission may reject the Home Secretary's opinion when it was "one which no reasonable minister advising the Crown could in the circumstances reasonably have held".⁵⁰⁰

The fact that judges have found that this deferential standard of determining injury to the broad concepts of international relations, national defence or national security has not been satisfied underlines the problems with the overclaiming of secrecy discussed above.

The third step requires the judge to determine whether the public interest in disclosure outweighs the public interest in non-disclosure. At this stage, "the party seeking disclosure of the information bears the burden of proving that the public interest is tipped in its favour."⁵⁰¹ Here the Court of Appeal discussed two possible standards, one that required the accused to establish a fact crucial to its case,⁵⁰² and another more restrictive standard requiring the accused to establish that his or her innocence was at stake.⁵⁰³ The Court of Appeal expressed some preference for the more restrictive latter test, given the similarities between the protection of informers and the safety of the nation, but applied the former test because it was more favourable to the accused and had been applied by Blanchard J.⁵⁰⁴ The Court of Appeal concluded that Blanchard J. had committed no error either in applying the relevant tests. In particular, "the prohibition against the two witnesses to testify at the criminal trial was, in the circumstances, the only viable and efficient condition which would most likely limit any injury to national defence,

⁵⁰⁰ *ibid* at paras 18-19.

⁵⁰¹ *ibid* at para 21.

⁵⁰² As applied in *Jose Pereira E Hijos S.A. et al v. The Attorney General of Canada* [2002] F.C.J. no. 1658

⁵⁰³ As applied in *R. v. Leipert* [1997] 1 S.C.R. 281 and *R. v. Brown* [2002] 2 S.C.R. 185

⁵⁰⁴ *R. v. Ribic* [2003] F.C. no. 1964 at para 27

national security or international relations.”⁵⁰⁵ It should be noted that the Federal Court would generally apply either standard in a pre-trial setting where it may be difficult to know what facts are crucial to the case or what may indicate that innocence may be at stake.

4. The Matter Returns to the Criminal Trial Judge

In the bifurcated scheme established by s.38, trial judges have to accept the Federal Court’s judgment about what information can be disclosed and in what form, but they also have a complete freedom to fashion whatever remedy they determine is necessary to protect the accused’s right to a fair trial. Although now specifically codified in s.38.14, this system of checks and balances has long been in place. It was, for example, asserted in the Kevork case study discussed above.

The *Ribic* case returned to a new trial judge, Rutherford J., who decided a number of motions before eventually presiding over the trial and sentencing of the accused. Despite all the s.38 proceedings that had been taken in Federal Court in relation to disclosure, Rutherford J. had to deal with a late-breaking disclosure issue in relation to the disclosure of documents in seventeen boxes that were said to constitute the office of a military attaché in Belgrade. DND personnel had inventoried and examined every page of those documents, and had disclosed to the accused fifty four pages of documents that contained a number of key words relevant to the case, including the names of the accused, the victims, the place, the hostage-taking and the military capacity in the area. Rutherford J. rejected the accused’s request for a fuller inventory of the documents or the inclusion of additional key words on the basis that the Crown’s procedure had “established a prima facie basis for irrelevance”, and that it was “hard to imagine, without some basis being shown by the defence”, how the remaining documents could be relevant, concluding that the defence’s case “seems to me to be little more than a fishing exercise”.⁵⁰⁶

As the criminal trial judge, Justice Rutherford also dealt with the admissibility of the edited transcripts of the two governmental witnesses whose evidence was subject to protracted litigation and appeal in the Federal Court. In an oral judgment at the end of May, 2005, Rutherford J.

⁵⁰⁵ *ibid* at para 53

⁵⁰⁶ *R. v. Ribic* [2004] O.J. no 569 at para 14

dealt with the defence application to admit the transcripts of witnesses A and B when they gave *in camera* and *ex parte* testimony in the Federal Court. Rutherford J. admitted the transcripts, concluding that they constituted a principled exception to the rule against admitting hearsay statements that could not be cross-examined, on the basis that the edited transcripts were “sufficiently necessary and taken under circumstances supportive of its threshold reliability so that it may be so admitted.”⁵⁰⁷ He also relied on his powers to fashion a broad range of orders necessary to protect the fairness of the accused’s trial, while respecting Federal Court rulings about what evidence could be disclosed. Although the transcripts were admitted in this case, it should be stressed that they were used for evidence that the accused sought to introduce. The same procedure might be more difficult to justify, either as a reliable and necessary exception to the hearsay rule, or as consistent with the accused’s right to a fair trial, in a case in which the Crown sought to introduce transcripts of testimony that had been taken *ex parte* and *in camera* and had been edited to delete material that would adversely affect national security.

In any event, the defence argued a month later, after it had put its case to the jury, that the reading of the edited transcripts of witnesses A and B to the jury violated the rights to a fair trial and full answer and defence under ss.7 and 11(d) of the Charter and that the appropriate remedy was a stay of proceedings. Although he suggested that there was “some merit”⁵⁰⁸ to these submissions, Justice Rutherford held that no Charter violations had been established. He noted that the Federal Court, in the editing process, had applied a standard more favourable to the accused than the innocence at stake exception with respect to the disclosure of the identity of police informers. Moreover, he stressed that A and B had only provided evidence relating to the context of the hostage-taking, as opposed to the hostage-taking itself, and that there was no evidence that went against the testimony of A or B or that challenged their credibility. (B’s testimony related to the bombing procedures used by NATO, and A’s related to NATO consideration that Serb forces might use hostage-taking as their only feasible tactic to stop the bombing.) Justice Rutherford stated:

I have concluded that the limits as to A and B’s evidence complained of by the defence do not go so far as to

⁵⁰⁷ *R. v. Ribic* [2005] O.J. no 2628 at para 6. Justice Rutherford did refuse to qualify witness B as an expert, however, in part because of the inability to cross-examine witness B. *ibid* at para 16.

⁵⁰⁸ *R. v. Ribic* [2005] O.J. no. 2631 at para 26

render the trial constitutionally unfair. The accused relies on A and B's evidence for his defence and I think it was made available in a process of sufficient fairness in all the circumstances....A and B do not speak to the subjective and personal aspects of Mr. Ribic's individual role and activity in the hostage-taking. I might be more reluctant and hesitant to find that evidence going directly to such core issues of an offence, such as the identity of the accused or the extent of his participation in the *actus reus* of the offence, could be similarly limited without more seriously impairing the fair trial rights of the accused.⁵⁰⁹

This decision affirms the availability of creative means to reconcile the state's interests in secrecy with the accused's rights to full answer and defence. Nevertheless, reliance on edited transcripts might not be acceptable if the evidence was more centrally related to the crime. In this case, the accused was charged with the discrete crime of hostage-taking, and the judge could be satisfied that the witnesses in the edited transcripts were not giving evidence crucial to guilt or innocence. The same approach might not be available if the accused was charged with a less discrete terrorism offence. In such cases, relevant witnesses might more often be in a position to speak to whether the accused committed the crime. In such circumstances, a trial judge might be less willing to accept edited transcripts as opposed to live testimony and direct cross-examination. Justice Rutherford's consideration of this issue also indicates how the two court structure may result in a subsequent duplication of effort as the trial judge determines the admissibility of information that complies with the Federal Court order. Although s.38.06(4) of the CEA seems to contemplate that the Federal Court judge could permit evidence to be introduced in the subsequent criminal trial in a manner that does not comply with the ordinary rules of admissibility, the trial judge might, as Rutherford J. did, also consider the admissibility of the evidence.

5. Trial within a Reasonable Time Issues

Given all the motions and delays in this case, it was hardly surprising that the accused claimed that his right to a trial in a reasonable time had been violated and that proceedings should be stayed. In a June, 2004, decision, Rutherford J. charged almost a year of pre-trial delay to the Crown for failing to make prompt disclosure of material in its possession that was

⁵⁰⁹ *ibid* at para 36

relevant to the case. At the same time, he noted the difficulties of disclosure in cases that involve international investigations and intelligence:

In large and complex cases, particularly one such as this in which a large number of governments, international agencies and foreign personnel have been involved, some centrally and some most peripherally, satisfactory compliance with the duty to disclose can be very difficult to define.⁵¹⁰

Justice Rutherford next considered the delay from November, 2002, to April, 2004, when the Federal Court of Appeal eventually resolved the s.38 procedures with respect to the accused's application to have two military witnesses give testimony. Although noting that the Federal Court made "real efforts to deal with the issues put before them with dispatch", and that leaving such issues "in the hands of trial courts to deal with in the course of a criminal trial may not be sufficiently protective of national security interests", he commented that the s.38 scheme:

...is cumbersome, and in this case was destructive of the trial process then in mid-course...It would be hoped that a mistrial and similar delay would not automatically result in every such case, as experience leads to even greater effectiveness in dealing with this legislative scheme. While such proceedings may be rare, one cannot help but wonder whether in this world of increasing terrorism, we may not, sadly, have cause to increase our experience with such issues and procedures substantially. The importance of Canada being able to do these things and to make them work without throwing in the towel and saying that we have no capacity to administer criminal justice in cases where national security issues are at stake, cannot be overstated.⁵¹¹

Justice Rutherford stressed that the 20 months spent in Federal Court proceedings were in relation to evidence "said to be of great value and potential benefit to the accused, by his counsel". This suggests that he may have been less tolerant of the delay if the s.38 proceedings had been initiated by the Crown and not the accused.

⁵¹⁰ *R. v. Ribic* [2004] O.J. no. 2525 at para 32

⁵¹¹ *ibid* at para 49

In the end, Justice Rutherford found that the accused's s.11(b) rights were not violated by the total five-year delay. He reasoned that "the national and international interests in bringing this case to trial are great...even where the issues involving sensitive information require collateral and time-consuming proceedings in the Federal Court..."⁵¹² A year after this ruling, and after the Crown and defence evidence had gone before the jury, Rutherford J. dismissed another s.11(b) application. He recognized that "the six years between the charges and the trial in this case is beyond all normal guidelines and may be quite unprecedented". Nevertheless, he found that the balance of interest still favoured the conclusion that the right to a trial in a reasonable time had not been violated.⁵¹³ Although not amounting to a s.11(b) violation, the 6 years of delay in this case underlines the difficulties of prosecutions that involve intelligence and s.38 applications.

On June 12, 2005, the second jury convicted Mr. Ribic of two counts of hostage-taking by detaining but found him not guilty of hostage-taking by forcible seizing. He was subsequently sentenced to three years imprisonment.⁵¹⁴

6. Summary

Some might argue that the eventual verdict in the Ribic case, combined with the 2001 amendments to s.38 to encourage earlier notification of the Attorney General of Canada, affirm the viability of Canada's two-court approach to managing the relation between evidence and intelligence in criminal trials. Nevertheless the Ribic case was hardly an unqualified success, and the innovative procedures it employed may be less acceptable in a terrorism prosecution and less acceptable in cases where the accused is not attempting to introduce evidence that implicated secret information. Similarly, much of the delay caused by litigation in the Federal Court was charged against the accused because the accused sought to call governmental witnesses. In other more typical cases such as *Kevork* and *Khawaja* where it is the Attorney General of Canada who seeks a non-disclosure order under s.38, the delay would likely be charged against the Crown. The innovative procedure of allowing edited transcripts (of witnesses' replies to questions posed by a security-cleared

⁵¹² *ibid* at para 50

⁵¹³ *R. v. Ribic* [2005] O.J. No 2631. Only a few months of this further year were attributed to the Crown because of disclosure problems, with some of the delay being attributable to the accused because of its unsuccessful motion decided in December, 2004, for further disclosure.

⁵¹⁴ *R. v. Ribic* [2005] O.J. No. 4261

lawyer employed by the federal government) may not be found to be satisfactory in cases where the evidence is given on crucial issues at trial and not, as in Ribic, on more general issues of context.

Finally, Justice Rutherford's warnings that the two-court procedure required by s.38 "is cumbersome, and in this case was destructive of the trial process then in mid-course...It would be hoped that a mistrial and similar delay would not automatically result in every such case" should provide pause. He indicated that the importance of Canada being able to bring terrorism cases to verdict even though they often will involve intelligence "cannot be overstated."⁵¹⁵ As will be seen in the next case study, the litigation and appeal of issues under s.38 has caused significant delays in the prosecution of Canada's first case under the *Anti-Terrorism Act*.

H) Use of Section 38 Before a Criminal Trial: A Case Study of R v. Khawaja

Although the Ribic case discussed above tested some of the provisions of s.38 that were added in the 2001 *Anti-Terrorism Act*, the first test of the new legislation in the context of a terrorism prosecution has come in the Khawaja case. The case was commenced by the laying of multiple charges against Mohammad Momin Khawaja in March, 2004. Khawaja brought a partially successful pre-trial Charter motion before the trial judge with respect to the constitutionality of the various terrorism offences of which he was charged. This motion was decided in October, 2006, and the Supreme Court subsequently denied leave to hear an appeal from that pre-trial ruling.⁵¹⁶ The parties next engaged in proceedings under s. 38 of the Canada Evidence Act both with respect to its consistency with the Charter and with respect to the disclosure of about one thousand, seven hundred pages out of almost ninety-nine thousand pages of material that had been disclosed to the accused.⁵¹⁷

1. The Charter Challenge to Section 38

A constitutional challenge by the accused that s.38.11(2) infringed ss.2(b), 7 and 11(d) of the Charter was commenced in March, 2007, and

⁵¹⁵ *R. v. Ribic* [2004] O.J. no. 2525 at para 49

⁵¹⁶ *R. v. Khawaja* (2006) 214 C.C.C.(3d) 399 (Ont. Sup.Ct.)

⁵¹⁷ *Canada v. Khawja* 2007 FC 463 at para 10.

decided by Chief Justice Lutfy in late April, 2007. The impugned provision provides that the judge conducting the s.38 proceeding, and any judge hearing an appeal or review of an order under s.38.06, may give any person making representations and shall give the Attorney General of Canada “the opportunity to make representations *ex parte*.” Chief Justice Lutfy interpreted the Supreme Court’s judgment in *Charkaoui* to allow accommodations to be made for the national security context in terms of substitute measures for access to secret information while at the same time ensuring fundamental fairness.

The right to know the case to be met is not absolute. Canadian statutes sometimes provide for *ex parte* or *in camera* hearings in which judges must decide important issues after hearing from only one side. *Charkaoui* at para 57. In order to satisfy s.7, either the person must be given the necessary information or a substantial substitute for that information must be found. *Charkaoui* at para 61.⁵¹⁸

He then cited the ability of the judge to authorize partial disclosure under s.38.06(2); a “flexibility...not written into the version of section 38 which existed prior to the amendments enacted by the *Anti-Terrorism Act*”⁵¹⁹; the ability of the accused to make *ex parte* representations; the ability of the accused to appeal Federal Court decisions under s.38.06; and the ability of the trial judge under s.38.14 to order appropriate remedies in light of any non-disclosure order to protect the accused’s right to a fair trial, as all factors that supported the constitutionality of the *ex parte* provisions in s.38.11.

A final safeguard considered by Chief Justice Lutfy that supported the constitutionality of s.38 was the ability of the judge conducting a s.38 hearing to appoint an *amicus curiae* to challenge the government’s *ex parte* representations.

In my view, the Court’s ability, on its own initiative or in response to a request from a party to the proceeding, to appoint an *amicus curiae* on a case-by-case basis as may be deemed necessary attenuates the respondent’s concerns with the *ex parte* process. This safeguard, if and when it need be used in the discretion of the presiding

⁵¹⁸ Ibid at para 35.

⁵¹⁹ Ibid at para 39.

judge, further assures adherence to the principles of fundamental justice in the national security context.⁵²⁰

The details about how an *amicus curiae* would operate were left to the discretion of the presiding judge, and there was no apparent consideration of the alternative that was used in the Malik and Bagri case of disclosure to the accused's lawyer subject to undertakings not to share the information with the client.

The accused's appeal of this ruling was dismissed by the Federal Court of Appeal. Two of the judges concluded that s.38 proceedings did not even engage the right to liberty under s.7 of the Charter because they were preliminary to the criminal trial. Pelletier J.A. concluded for this majority that "the *ex parte* proceedings which subsection 38.11(2) authorizes do not raise issues of full answer and defence, and of knowing the case to be met. I am also inclined to the view that *ex parte* proceedings under subsection 38.11(2) do not engage Mr. Khawaja's liberty interest simply because those proceedings have no impact upon Mr. Khawaja's liberty interest, even though the product of those proceedings may do so."⁵²¹

This approach stresses a divide between the s.38 process and the ultimate criminal trial. It runs the risk of leaving the difficult issues of trial fairness to a trial judge who will not have seen the information that is subject to a Federal Court non-disclosure order and who will have no ability to revise that order. Even Richard C.J. who concluded that s.38 proceedings affected the accused's liberty interests stressed the ability of the trial judge to protect the accused's fair trial rights when he stressed that "the judge presiding at a criminal proceeding has further powers under section 38.14 of the *Canada Evidence Act* to protect the right of an accused to a fair trial by making (a) an order dismissing specified counts of the indictment or information, or permitting the indictment or information to proceed only in respect of a lesser or included offence; (b) an order effecting a stay of proceedings; and (c) an order finding against any party on any issue relating to information the disclosure of which is prohibited."⁵²² The emphasis that the Federal Court of Appeal accorded to the ability of the trial judge to orders remedies under s.38.14 to protect the accused's right to a fair trial reflects the division of labour between the two courts, but does not respond to the fact that the trial judge will have a limited range

520 Ibid at para 59

521 *Canada v. Khawaja* 2007 FCA 388 at para 117

522 Ibid at para 46-48

of blunt and often drastic remedies available to protect the fairness of the trial. The trial judge cannot re-visit a non-disclosure order made by the Federal Court and may have little choice but to stay proceedings, or stay proceedings in relation to a particular charge, if the trial judge is concerned that the non-disclosure of information adversely affects the accused's right to full answer and defence.

Even assuming that the accused's right to liberty was engaged by the s.38 process, all the judges concluded that the *ex parte* proceedings complied with the principles of fundamental justice or were capable of justification under s.1 of the Charter. They stressed the importance of protecting secret intelligence and the dangers of disclosure to the accused. Richard C.J. stressed that any concerns about the relevance of the material to the accused's defence could be addressed by the ability of the accused to make *ex parte* submissions to the Federal Court to inform him or her of "the theory of the defence".⁵²³ Pelletier J.A. held that *ex parte* proceedings were justified in part by concerns about the mosaic effect discussed above. He stated:

The difficulty in deciding whether information, apparently innocuous on its face, has value to a hostile observer goes a long way towards explaining Parliament's decision to authorize *ex parte* submissions by the Attorney General. In order to permit the Attorney General to address the Court candidly without worrying about disclosing information whose disclosure, it is alleged, would be injurious to Canada's legitimate interest in her national security, Parliament authorized the Court to receive *ex parte* evidence and submissions from the Attorney General.⁵²⁴

Pelletier J.A. concluded that without *ex parte* proceedings, the government would only be able to speak in generalities about the information that was the subject of s.38 proceeding. "The absence of Mr. Khawaja means that the Attorney General can speak freely and specifically of the risks of disclosure but more importantly, the applications judge can ask specific questions and expect specific answers. None of this is possible if the judge and counsel for the Attorney General are required to speak at a level of generality which precludes full disclosure and close questioning

⁵²³ Ibid at para 39.

⁵²⁴ Ibid at para 124.

by the judge hearing the application.”⁵²⁵ *Ex parte* proceedings that allow the judge, perhaps assisted with a security cleared special advocate, to see the secret material and question the government’s lawyer may well be required, but the issue is whether such hearings would be best held before the Federal Court or the trial judge. A trial judge who conducted such hearings would have the option of revising the initial non-disclosure as well as ordering the remedies contemplated under s.38.14.

2. Two Rounds of Section 38 Hearings and an Appeal

Litigation was also conducted under s.38 with regard to what information should be disclosed to the accused. The Attorney General of Canada sought non-disclosure of five hundred and six documents from the RCMP, CSIS and Canadian Border Services Agency, including material that they had received in confidence from foreign agencies. These five hundred and six documents consisted of several thousands of pages, of which seventeen hundred pages had redacted information.⁵²⁶ At the same time, they constituted only two percent of the almost ninety-nine thousand pages that had been disclosed to the accused, including two hundred and twenty-six cd’s of intercepted conversations, thirteen surveillance tapes and various surveillance records. The accused made “clear that he is not seeking the disclosure of information that would reveal sensitive investigative techniques, the identity of any undercover operatives of law enforcement and/or intelligence agencies, or the targets of any other investigation.”⁵²⁷

Justice Mosley released a judgment outlining the principles and procedures to decide the merits of the Attorney General’s non-disclosure application under s.38 of the CEA. This judgment described the undisclosed material as consisting of about three hundred and fifty documents that dealt with internal administrative matters, two hundred and sixty documents that dealt with operational methods, and one hundred and thirty-eight documents about ongoing investigations into other targets. He noted that the accused did not even seek disclosure of those types of information.⁵²⁸

About one hundred and forty documents related to information received in confidence from foreign third parties. They included an intelligence

⁵²⁵ Ibid at para 139.

⁵²⁶ *Attorney General of Canada v. Khawaja* 2007 FC 490 at paras 5, 31

⁵²⁷ *Attorney General of Canada v. Khawaja* 2007 FC 490 at para 8.

⁵²⁸ Ibid at para 44

report that had not been disclosed in the British trials. The originating foreign intelligence agency refused to consent to the disclosure of this intelligence report. Justice Mosley reviewed the intelligence report and concluded that it was “not evidence that will be used against the accused, nor does it go to exculpate him or to undermine the Crown’s case.”⁵²⁹ This suggests that undisclosed intelligence may not always have evidentiary value or be useful to the accused. The conclusion that the undisclosed intelligence does not exculpate the accused or undermine the Crown’s case applies a more restrictive standard than would normally be applied under *Stinchcombe*.

Some of the undisclosed material included abstracts of the FBI’s interview of a potential key witness in the Khawaja case. The FBI did not consent to disclosing this material because it contained material relating to ongoing operations. The FBI did, however, substitute an unclassified ninety-nine-page report of the information that they obtained from the witness. After reviewing both classified and unclassified versions, Justice Mosley concluded that the differences “are not, in my view, material.”⁵³⁰ He noted the accused’s interest in knowing what consideration this witness received from American officials, but concluded that there was no information about any payments to the potential witness in any the disputed material.⁵³¹ In addition, at the court’s direction, Canadian officials obtained a new consent from American officials to agree to the release of the plea agreement with the potential witness.⁵³² Thus, substitutions and consent to disclose were obtained with respect to documents that American officials would initially not consent to disclose. As suggested above, this supports a more flexible approach to the third party rule in which Canadian agencies will seek consent from foreign agencies to the disclosure of information.

The judgment was followed by a public and a private order specifying that some of the information need not be disclosed because it was not relevant to the criminal proceeding, but that 67 documents should be fully or partially disclosed.⁵³³ The confidential summary could be of use to the trial judge if it provides the trial judge with a better sense of what material was not disclosed and its potential effect on the accused’s right to a fair trial and full answer and defence. That said, the Federal Court of Appeal

529 *ibid* at para 50

530 *ibid* at para 55

531 *ibid* at para 177

532 *ibid* at para 57.

533 Public Order May 17, 2007 DES-2-06

subsequently determined that Justice Mosley had erred by including descriptive information in the schedule of undisclosed documents that would injure national security.⁵³⁴

Justice Mosley noted that some of the non-disclosures made by the Attorney General were not properly brought under s.38 because they involved claims of common law privileges or specified public interest immunities under s.37 of the CEA. Such issues would have to be decided by the trial judge.⁵³⁵ Although the designated judge has a limited mandate under s.38, the division of labour raises concerns about the efficiency of the process. Decisions about disclosure decided by the Federal Court judge under s.38 of the CEA could potentially be re-litigated before the trial judge under s.37 and under the common law, if the Crown chose to reformulate its legal claims for non-disclosure.

Justice Mosley applied the three part test outlined by the Federal Court of Appeal in the *Ribic* case discussed above. Despite recognition that the first requirement under *Stinchcombe*, that the documents be relevant, was a low threshold, and that the prosecutor had conceded the relevance of the undisclosed material, Justice Mosley concluded that some of the material was simply not relevant to the case and need not be disclosed on that basis. He included "in the irrelevant category analytical reports of a general nature, some of which were prepared years before the events that gave rise to the charges against the respondent and are not specific to the context of those charges."⁵³⁶ This decision, combined with similar ones made in *Ribic*, underlines that analytical and general intelligence may, in some cases, simply not be relevant information that has to be disclosed. It also raises concerns that prosecutors may be prepared to disclose irrelevant material that does not have to be disclosed under *Stinchcombe*.

In applying the second step of whether the disclosure of the information would harm national security or international relations, Justice Mosley was presented with information that stressed that Canada was a net importer of intelligence, including an estimate by a RCMP officer that Canada imports

⁵³⁴ *Attorney General v. Khawaja* 2007 FCA 342 at para 12.

⁵³⁵ *Attorney General of Canada v. Khawaja* 2007 FC 490 at para 34

⁵³⁶ *ibid* at para 116. The accused's argument on appeal that the s.38 judge should accept relevance as determined by the prosecutor's application of *Stinchcombe* was rejected on the basis that the Federal Court judge had an independent obligation to determine whether the material was relevant. *Attorney General of Canada v. Khawaja* 2007 FCA 342 at paras 23-25.

intelligence on a factor of 75:1.⁵³⁷ As discussed above, he indicated that the Attorney General could not claim the protection of the third party rule if it had not requested the foreign agency to consent to disclosure, or if the information was received from CSIS as opposed to a foreign agency, or if the information was publicly available.⁵³⁸ As discussed above, this approach demonstrates an appropriate recognition that caveats placed on the disclosure of information can be amended, and that the third party rule should not be applied in a rigid or mechanical fashion to thwart disclosure. He ordered some documents to be fully disclosed on the basis that their disclosure would not cause injury to international relations or national security.⁵³⁹ Such a conclusion that the harm of disclosure has not been established raises concerns about the overclaiming of national security confidentiality, especially given the deferential standards that judges apply in determining whether the disclosure of information will cause harm to national security or international relations and the breadth of the harms encompassed by those terms.

With respect to the third stage, Justice Mosley noted that the accused had the onus of demonstrating that the public interest in disclosure outweighed the public interest in non-disclosure. He stated that while the accused's "fair trial rights are an important factor, I do not accept that they 'trump' national security or international relations in every case particularly where, as here, it is not at all clear that there would be any infringement of the right to make full answer and defence by non-disclosure of this information."⁵⁴⁰ He noted that the accused had not revealed to the Court what his defences would be or made *ex parte* submissions to him. He reconciled the competing public interest in non-disclosure and in disclosure, given the serious charges faced by the accused, by making use of summaries of information that, if disclosed, would harm national security or international relations.⁵⁴¹ In the end, he ordered that sixty-seven of the five hundred and six documents be disclosed or summarized for the accused.

The Federal Court of Appeal allowed the government's appeal, only to the extent that some of the information that Justice Mosley revealed in

⁵³⁷ *ibid* at para 127

⁵³⁸ *ibid* at paras 146-150.

⁵³⁹ For another decision apparently holding that some of the information that the government claimed did not satisfy the injury test see *Canada v. Commission of Inquiry into the actions of Canadian Officials in Relation to Maher Arar* 2007 FC 766 at para 91.

⁵⁴⁰ *Ibid* at para 166

⁵⁴¹ *ibid* at para 186

his schedule describing items that were not to be disclosed had the effect of disclosing information that should not have been disclosed. The Court of Appeal rendered its judgment two weeks after hearing the appeal, and noted that all efforts had been made to proceed expeditiously in the interests of justice.⁵⁴² Pelletier J.A. concurred in the result, but held that the more expeditious and proper method of proceeding would have been for the Attorney General of Canada to have returned to Justice Mosley for a clarification of his ruling.⁵⁴³

The Court of Appeal rejected the accused's non-constitutional appeal, holding that Justice Mosley was entitled to order the non-disclosure of information that did not have to be disclosed under *Stinchcombe* even though the prosecutors in the case had conceded that the material was relevant under *Stinchcombe*. The Court of Appeal also indicated that, as part of discharging its burden to establish the case for disclosure, the accused should have made *ex parte* submissions under s.38.11(2). Letourneau J. A. stated:

Obviously, the right to full answer and defence when facing serious criminal charges is a highly relevant consideration in balancing the competing public interests. However, in order to make a meaningful review of the information sought to be disclosed, the judge must be either informed of the intended defence or given worthwhile information in this respect.⁵⁴⁴

In that case, the accused had apparently made a tactical decision not to make *ex parte* submissions that would explain the defence. Even in the absence of such a tactical decision, the accused would have difficulty arguing that information that he had not seen was critical to his defence.

The accused sought leave to appeal this decision to the Supreme Court of Canada, but it was denied.⁵⁴⁵ This appeared to set the stage for the

⁵⁴² Letourneau J. A. stated: "I should say at the beginning that the reasons for judgment will be succinct. The respondent is in custody. He is awaiting his trial in the Ontario Superior Court of Justice on seven criminal charges relating to a conspiracy to commit terrorist acts in the United Kingdom. At the request of counsel for the respondent, the hearing of this appeal has been adjourned once. In the interest of justice, which includes those of the respondent, all efforts have been made to proceed expeditiously to render a decision." *Canada. v. Khawaja* 2007 FCA 342 at para 6.

⁵⁴³ *Canada. v. Khawaja* 2007 FCA 342 at paras 50-51.

⁵⁴⁴ *ibid* at para 35.

⁵⁴⁵ April 3, 2008 per McLachlin C.J.C., Fish and Rothstein JJ.

commencement of the trial. In early 2008, however, the Attorney General of Canada served a number of notices that it would be seeking non-disclosure orders in fresh s.38 proceedings in relation to 32 documents held by the RCMP. Issues of late disclosure frequently arise in long and complex trials, but the fresh round of s.38 litigation caused the trial judge, Justice Rutherford, to raise the question of whether it is possible to conduct trials involving issues of national security confidentiality; comments similar to those the same experienced trial judge had made in relation to the *Ribic* case study examined above.⁵⁴⁶ Indeed, it is still possible that more s.38 issues may emerge at trial if, for example, the accused seeks to call witnesses from Canada, the United States or the United Kingdom who may have access to secret information.

In the second round of s.38 proceedings, the Federal Court appointed a security-cleared *amicus curiae* and two days of hearing were held in April, 2008 on the matter. On April 29, 2008, the Attorney General of Canada advised the court that it had authorized the disclosure of some of the disputed documents in unredacted form in part because a foreign agency had agreed to the release of the information that had been provided under caveat.⁵⁴⁷ The next day, Justice Mosley issued a ruling holding that the remaining documents which dealt with administrative matters and communications with foreign agencies need not be disclosed. These documents did not satisfy the threshold test of relevance because they “would not be of assistance to the defence in the underlying criminal proceedings and does not meet the low threshold of relevance”⁵⁴⁸ which was equated with the *Stinchcombe* standard of material that was not clearly irrelevant.⁵⁴⁹

Justice Mosley added that had he been required to consider the next stage of the three-part *Ribic* analysis, he “might have found that the Attorney General had not met his burden of establishing that disclosure of some of the redacted information would cause injury to the protected interests. As I have previously noted, there tends to be an excessive redaction of innocuous information in these cases.”⁵⁵⁰ This decision is noteworthy in confirming a persistent practice in this case of the Attorney General overestimating the demands of disclosure under

⁵⁴⁶ Ian MacLeod “Terror trial delay angers judge Provincial magistrate in Khawaja case frustrated by interference from Federal Court” *The Ottawa Citizen* Jan 25, 2008.

⁵⁴⁷ *Canada v. Khawaja* 2008 FC 560

⁵⁴⁸ *Ibid* at para 14

⁵⁴⁹ *Ibid* at paras 9-10.

⁵⁵⁰ *Ibid* at para 14.

Stinchcombe and bringing s.38 proceedings with respect to information that was subsequently determined did not need to be disclosed because the information was not relevant to the accused even under the broad *Stinchcombe* standards of disclosure. That said, it is also possible that the Federal Court is applying a more restrictive reading of *Stinchcombe* than those prosecuting the case are used to being applied in criminal courts. In any event, the decision also suggests that the Attorney General again claimed national security confidentiality in a case where the reviewing judge was not convinced that disclosure of the information would even cause harm to national security, despite the deference that judges give to the executive on this issue and the broad nature of possible harms to national security.

This decision also contains some interesting procedural innovations. It suggests that the Federal Court is prepared to use security cleared special counsel to provide adversarial argument on s.38 issues that arise in connection to a criminal trial and that this can be done in an expeditious manner. The security cleared counsel was appointed on April 3, 2008 and participated in hearings on the s.38 matter on April 15, and 18, 2008.⁵⁵¹ It is not known whether the security cleared lawyer had access to the voluminous disclosure in this case or what, if any, contact he had with the accused and his lawyer before or after examining the secret information that was the subject of the s.38 application. Justice Mosley remained seized of the matter pending the outcome of the criminal trial and indicated that the parties could seek “clarification” of his order at any time. In this case, Justice Mosley did not prepare a detailed schedule of the material subject to the non-disclosure order because he determined that it was largely clear what material was subject to the non-disclosure order and the material was not relevant in any event.⁵⁵² In more difficult cases, however, the accused could be at a disadvantage in seeking any clarification of the order having not seen the information.⁵⁵³ It is not clear whether the security cleared lawyer would continue to play a role at trial.

Even if this decision is not appealed to the Federal Court of Appeal and if it represents the final round of s.38 litigation, the Attorney General and the accused could continue to fight similar battles before the trial judge. The Attorney General of Canada would be able to claim specified public interest

⁵⁵¹ Ibid at para 6.

⁵⁵² Ibid at para 17.

⁵⁵³ In this case, the accused's lawyers had actually seen seven of the documents because of inadvertent disclosure. This material was the subject of a continuing non-disclosure order. Ibid at para 16.

immunities under s.37 of the CEA and the common law before the trial judge. This could potentially allow issues about the protection of sources and witnesses and intelligence and police methods of investigation to be re-litigated in cases where the Federal Court had rejected a case for a non-disclosure order under s.38. Even if this was not done, it is almost certain that the accused will argue before the trial judge that a remedy, including a stay of proceedings, should be ordered under s.38.14 of the CEA in order to protect the right to a fair trial.⁵⁵⁴ It is not clear what, if any, role that the security cleared lawyer appointed in *Khawaja* could play in such proceedings. This security cleared lawyer would be bound not to disclose secret information to the trial judge. Justice Mosley's provision of a confidential schedule of non-disclosed items may put the trial judge in a more informed position to decide whether a fair trial is still possible in light of the non-disclosure order, but some of the information included in this schedule will be deleted as a result of the Federal Court of Appeal's decision that its release would harm national security. Justice Mosley did not order a similar schedule in the second round of the s.38 litigation, but he remained seized of the matter and indicated that he could "clarify" the order on a motion by the parties. This opens up the possibility that an order could be amended in response to changed circumstances in the trial, but both the accused and trial judge would still not have access to the information subject to the non-disclosure order.

The prospects of continued and protracted disputes over the non-disclosure of information raises questions about the workability of the unique two-court system that Canada uses to resolve claims of national security confidentiality. Mr. Khawaja's alleged co-conspirators in Britain were tried before Khawaja's trial had even started in Canada. He was charged in 2004 and 1,492 days elapsed between the charge and the latest decision under s.38 of the Canada Evidence Act.⁵⁵⁵ The British terrorism trial started in March, 2006 and was completed by the end of April, 2007 despite the fact that the British trial was long and involved nearly a month of jury deliberations.⁵⁵⁶ The Canadian trial has not started as of the end of April, 2008. As will be seen in the next section, issues of national security confidentiality in Britain are decided by the trial judge.

⁵⁵⁴ The trial judge will not have access to the documents that are not disclosed but Justice Mosley's order contemplates that he or she may have access to the private order and schedule that presumably provides more detail than the public order about what has been disclosed and not disclosed. *Attorney General of Canada v. Khawaja* Public Order May 17th, 2007 at para 7.

⁵⁵⁵ Ian MacLeod "Ruling Clears Way for Khawaja Trial" *Ottawa Citizen* May 2, 2008.

⁵⁵⁶ Doug Saunders "Long list of strange delays plagued court" *Globe and Mail* May 1, 2007 p.A-15.

I) Summary

Attitudes towards national security confidentiality have evolved considerably over the last twenty-five years. Until 1982, a federal Minister could assert an unreviewable claim to protect information on national security grounds. Courts were reluctant even to examine such material.⁵⁵⁷ There was considerable concern that the disclosure of even innocuous information could harm national security, national defence and international relations through the mosaic effect because of the abilities of Cold War adversaries to put together the pieces of information.⁵⁵⁸ In recent years, however, courts are more cautious about claims of the mosaic effect, and have indicated that Canada should seek permission from allies to allow the disclosure of information under the third party rule.⁵⁵⁹ Concerns have been raised that the overclaiming of national security confidentiality causes delays and creates cynicism about legitimate secrets.⁵⁶⁰ The third party rule remains a critical component of legitimate claims of national security confidentiality, especially given Canada's status as a net importer of intelligence, but it should not be invoked in a mechanical manner. It only applies to information that has been received in confidence from a third party and should not be stretched to apply to information that either was in the public domain or was independently possessed by Canadian agencies. Canadian agencies should also generally seek the consent of the originating agency to the use of information covered by the third party rule.

The 2006 RCMP/CSIS MOU contemplates the use of s.38 of the CEA as a means to protect intelligence passed from CSIS to the RCMP from disclosure in criminal and other proceedings. Nevertheless, s.38 imposes a time- consuming and awkward process for reconciling the need for disclosure with the need for secrecy. Section 38 applies to a very broad range of information, and thought should be given to narrowing the range of information covered by s.38 and to specifying with much more precision the harms that can be caused by the disclosure of secret information. The Senate Committee reviewing the ATA has recommended that the harms to international relations be enumerated more precisely.

⁵⁵⁷ *Re Goguen* (1984) 10 C.C.C.(3d) 492 at 500 (Fed.C.A.).

⁵⁵⁸ *Henrie v. Canada* (1988) 53 D.L.R.(4th) 568 at 580, 578 affd 88 D.L.R.(4th) 575 (Fed.C.A.).

⁵⁵⁹ *Canada v. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* 2007 FC 766; *Canada v. Khawaja* 2007 FC 490.

⁵⁶⁰ *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar Report of the Events Relating to Maher Arar Analysis and Recommendations* (Ottawa: Public Works and Government Services) at pp 302, 304.

Such a harm-based approach could also be applied to the vague terms “national security” and “national defence”.⁵⁶¹ In other words, s.38 could be amended to specify the harms of disclosure to vulnerable sources and informers, to ongoing operations and methods of operation and with respect to undertakings given to foreign partners. Providing specific examples of harms to national security and international relations could help discipline the process of claiming national security confidentiality and respond to the problem of overclaiming secrecy. In addition, it appears from both the *Ribic* and *Khawaja* prosecutions that prosecutors need to be reminded that they need not seek s.38 non-disclosure orders if the information is clearly irrelevant to the case and can be of no assistance to the accused.

The ability of the Attorney General to make *ex parte* representations to the s.38 judge is only partly compensated for by the ability of the accused to make *ex parte* representations. The value of the accused’s *ex parte* representations will be attenuated by the fact that the accused has not seen the secret information that is the subject of the dispute. Several decisions by the Federal Court Trial Division⁵⁶² have opened up the possibility of appointing an *amicus curiae* who, unlike the accused’s lawyer, will be able to see the information and provide adversarial challenge to the *ex parte* submissions made by the Attorney General for non-disclosure. The use of such security cleared lawyers has not yet been approved by the Federal Court of Appeal.⁵⁶³ In any event, the appointment of such a person could delay the proceedings because that person will need to become familiar with the material that has already been disclosed to the accused and the possible uses that the accused might have for the undisclosed information. A special advocate or other security cleared lawyer will never be as familiar with the accused’s case and the possible uses of the undisclosed information as the accused’s

⁵⁶¹ The vagueness of the term national security is notorious. My colleague M.L. Friedland, for example, prefaced a study for the McDonald Commission with the following statement: “I start this study on the legal dimensions of national security with a confession: I do not know what national security means. But then, neither does the government.” M.L. Friedland *National Security: The Legal Dimensions* (Ottawa: Supply and Services, 1980) at 1.

⁵⁶² *Canada v. Khawaja* 2007 FC 463; *Khadr v. The Attorney General of Canada* 2008 FC 46; *Canada v. Khawaja* 2007 F.C. 560.

⁵⁶³ In upholding the constitutionality of s.38, the Federal Court of Appeal made no mention of the ability of appoint security cleared lawyers to assist in such proceedings. *Khawaja v. Attorney General of Canada* 2007 FCA 388 at para 135. In his concurring judgment, Pelletier J.A. cast doubt on the ability of the court to order that secret information be disclosed to even a security-cleared lawyer when he concluded that under s.38.02 that “the Court could not order and the Attorney General could not be compelled to provide, disclosure of the Secret Information to Mr. Khawaja, or anyone appointed on his behalf in any capacity.” *Ibid* at para 134.

own lawyers, but may play a valuable role in providing an adversarial challenge to the government's claim for secrecy.

Although the Federal Court has been given explicit flexibility under s.38.06 in reconciling competing interests in secrecy and disclosure, including editing and summarizing information, as was done in *Khawaja*, creating substitutes for classified information, such as the edited transcript used in *Ribic*, and making findings against the parties, the ultimate effect of these orders will depend on the judgment made by the criminal trial judge under s.38.14 about the effects of the non-disclosure order on the accused's right to a fair trial. There is a danger that the Federal Court judge may not be in the best position to know the value of information to the accused, given that the accused will not have access to the information and the trial often will not have started. In turn, there is a danger that the criminal trial judge may not be in the best position to know the effects of the non-disclosure of information on the fairness of the trial when he or she will not have seen the information. There is no specific mention, in either the Attorney General's powers under s.38.03 or the Federal Court judge's powers under s.38.06, of an ability to make an exception to a non-disclosure order that would allow a trial judge to see the undisclosed information. The blind spots of both the Federal Court judge and the trial judge run the risk of causing stays of proceedings that are not necessary in order to protect the fairness of the trial as well as trials that are not fully fair, and that could even result in wrongful convictions, because of the non-disclosure of information that the Federal Court and trial judges did not realize was necessary for the accused to make full answer and defence.

Although an innovative approach was devised between counsel in the Malik and Bagri prosecution in order to avoid Federal Court proceedings, the ultimate dispute resolution process when no agreement is reached involves separate proceedings in Federal Court. Section 38 proceedings will delay and fragment the criminal trial as seen in the *Kevork*, *Ribic* and *Khawaja* case studies discussed above. They will also not resolve all the disputes, as the Attorney General can still claim common law privileges and invoke s.37 of the CEA. In turn, the accused will seek a remedy for partial or non-disclosure under s.38.14 of the CEA when the matter returns to the trial judge. As will be seen, other democracies have not duplicated Canada's unique and cumbersome two-court process for resolving national security confidentiality claims.

VII. Disclosure and Secrecy in other Jurisdictions

In what follows, I will outline the approach used to resolve national security confidentiality claims in the United States, the United Kingdom and Australia. In all of these democracies, the criminal trial judge decides questions of national security confidentiality that in Canada are reserved to the Federal Court. In addition, I will examine provisions in other jurisdictions for requiring defence lawyers to obtain security clearances as a prerequisite to the viewing of sensitive material, as well as the role played by security-cleared special advocates or *amicus curiae* to challenge the government's case that secret intelligence need not be disclosed to the accused.

United States

1. Disclosure Requirements

Material held by intelligence agencies and classified as secret security intelligence may be subject to constitutional and statutory disclosure standards in the United States. The main constitutional case is *Brady v. Maryland*⁵⁶⁴ which held that "the suppression by the prosecution of evidence favorable to the accused upon requests violates due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution."⁵⁶⁵ An associate general counsel of the CIA has written that "close coordination between the activities of law enforcement and intelligence agencies in a particular matter should subject the intelligence files to *Brady* search."⁵⁶⁶ Other disclosure requirements relate to material that can be used to impeach a government witness, statements made by the accused, and documents or tangible objects that are material to the defence, belong to the accused or are intended to be used by the prosecution.⁵⁶⁷ Material subject to disclosure under either constitutional or statutory standards could, however, be the subject of an application for a non-disclosure order on the basis of national security concerns.

⁵⁶⁴ 373 U.S. 83 (1963)

⁵⁶⁵ *Ibid* at 87

⁵⁶⁶ Jonathan Fredman "Intelligence Agencies, Law Enforcement and the Prosecution Team" (1998) 16 Yale Law and Policy Review 331 at 354. But for a more limited approach to the search of an intelligence agency's files for exculpatory material see Mark Villaverde "Structuring the Prosecutor's Duty to Search the Intelligence for Brady Material" (2003) 88 Cornell L. Rev. 1471.

⁵⁶⁷ Fred Manget "Intelligence and the Criminal Law System" (2006) 17 Stanford Law and Policy Rev. 415 at 423.

2. Classified Information Procedures Act

In 1980, the United States enacted the *Classified Information Procedures Act*⁵⁶⁸ (CIPA) to provide procedures for pre-trial determinations of national security confidentiality. Before that time, many believed that it would be impossible to prosecute spies because it would result in the disclosure of classified information. Since 1980, however, CIPA has been successfully used in many successful espionage and terrorism prosecutions.⁵⁶⁹ Although CIPA has already influenced the 2001 amendments to s.38 of the CEA, it still provides a relevant example for further law reform that would allow trial courts to resolve issues of national security confidentiality. Like s.38 of the *Canada Evidence Act*, CIPA defines the information covered by it broadly, to include classified information that the government is taking steps to protect for reasons of national security. National security is also defined broadly, to include considerations of national defence and international relations. Section 5 of CIPA, like s.38.01 of the CEA, places robust requirements on the accused to notify both the United States attorney and the court before trial if they expect to disclose, or cause the disclosure of, classified information. Section 5(2), however, specifically provides that the court may preclude disclosure and prohibit the examination of witnesses as a sanction for failure to disclose. Although such sanctions are contemplated in the statute, their use could adversely affect the accused's constitutional right to make full answer and defence and a fair trial.

A noteworthy feature of CIPA, as compared to the CEA, is that the notice is given not only to United States Attorney but also to the trial court. CIPA contemplates that national security confidentiality claims can be managed by the trial judge as part of the case management and discovery process. To this end, section 2 of CIPA allows any party after the filing of the indictment or information, or the court on its own motion, to convene a pre-trial conference to establish the timing of requests for discovery, notices and hearings about national security confidentiality and any other "matters which relate to classified information or which may promote a fair and expeditious trial".⁵⁷⁰ In Canada, national security confidentiality issues would be delegated to the Federal Court and as such segregated from general pre-trial management in the criminal courts.

⁵⁶⁸ PL 96-456

⁵⁶⁹ Serrin Turner and Stephen Schulhofer *The Secrecy Problem in Terrorism Trials* (New York: Brennan Center, 2005).

⁵⁷⁰ CIPA s.2 (emphasis added)

3. Security Clearances for Defence Lawyers

One of the core dilemmas of national security confidentiality is that the process of determining whether the government has made a legitimate claim of secrecy may itself sacrifice secrecy. Section 3 of CIPA protects this anticipatory interest in confidentiality by providing that, upon a motion of the United States, “the court shall issue an order to protect against the disclosure of any classified information disclosed by the United States to any defendant in any criminal case in a district court in the United States.” Although CIPA on its face does not contemplate that courts can require defence lawyers to obtain security clearances as a prerequisite to obtaining access to classified information, courts have found this power is an incident to CIPA’s procedures. In *United States v. Bin Laden*⁵⁷¹, Judge Sands found authority to order security clearances for defence lawyers from security procedures promulgated by the Chief Justice of the United States under s. 9 of CIPA that allowed the government to use “lawful means” to obtain information “concerning the trustworthiness of persons associated with the defence” and to bring such information to the court’s attention for the purpose of framing an appropriate protective order under s.3 of CIPA.⁵⁷²

Judge Sands rejected constitutional challenges to the security clearance process on the basis that it did not necessarily give the Department of Justice a veto over the accused’s choice of lawyer.⁵⁷³ He also noted that similar requirements were imposed on court staff who had access to the classified documents.⁵⁷⁴ He also stressed that the government’s concerns about preventing leaks of classified information:

are heightened in this case because the Government’s investigation is ongoing, which increases the possibility that unauthorized disclosures might place additional lives in danger. In addition, the Government has alleged that the Defendants are part of a conspiracy whose members have previously gained access to un-filed

⁵⁷¹ 58 F.Supp.2d 113. To the same effect see *United States v. Al-Arian* 267 F.Supp. 2d 1258.

⁵⁷² *ibid* at 116 citing 18 U.S.C.A. app 3 s.9 (West, 1999) and distinguishing earlier cases holding that the notice requirements in s.5 of CIPA did not authorize requiring defence lawyers to undergo a security clearance. *United States v. Jolliff* 548 F.Supp. 232 (D.Md.1981); *United States v. Smith* 706 F.Supp. 593 (M.D. Tenn. 1989).

⁵⁷³ Early commentary had raised concerns that “to eliminate a particularly troublesome opponent, the Justice Department may deny a security clearance to a specific attorney, investigator, or expert witness retained by the defendant, who needs access to classified information to be effective.” Brian Tamanaha “A Critical Review of The Classified Information Procedures Act” (1986) 13 Am. J. Crim. L. 277 at 289.

⁵⁷⁴ Such requirements were upheld in *United States v. Smith* 899 F. 2d 564 (6th Cir, 1990).

court documents and forwarded those documents to other members of the conspiracy....Our insistence that every person who comes into contact with classified information in this litigation undergo some objective evaluation is, of course, no commentary on the reputations of the Defence counsel in this case. The fact remains that it is practically impossible to remedy the damage of an unauthorized disclosure ex post and we refuse to await the possibility of repairing what in this case might be a particularly disastrous security breach when reasonable measures could have prevented the disclosure altogether. We believe it is appropriate to require some form of clearance on the facts we have before us.⁵⁷⁵

As will be seen, Australian legislation explicitly contemplates that defence lawyers may require security clearances in order to gain access to classified information.

Although requirements that defence lawyers receive security clearances as a prerequisite to viewing classified material can adversely affect choice of counsel, it does have some advantages. In the Malik and Bagri trial, defence lawyers were able to inspect CSIS material on an initial undertaking that it not be disclosed with their client, but they did not receive security clearances. A defence lawyer with a security clearance may be able to participate more effectively in proceedings about classified information than a security-cleared special advocate or *amicus curiae*, who will inevitably not be as familiar with the case as the accused's own lawyer.

At the same time, however, the defence may be adversely affected if the security-cleared defence lawyers cannot consult with their clients. In a 2001 ruling in the Bin Laden case, Judge Sands was confronted with an argument that a security-cleared lawyer's inability to share classified information with his client denied the accused the effective assistance of counsel. The accused argued that they were severely handicapped in not being able to consult with their counsel because of "the length of the alleged conspiracies, their geographical scope, the language barriers, the myriad names (some very similar) and aliases, and the cultural and ethnic

⁵⁷⁵ 58 F.Supp.2d 113 at 121.

diversity involved”.⁵⁷⁶ Judge Sands rejected this claim, noting that some of the information under dispute was being declassified so it could be shared with the accused. Moreover, “the hypothetical benefit” of being able to share all classified information with the accused was outweighed by the “government’s compelling interest in restricting the flow of classified information”.⁵⁷⁷ Judge Sands also cited in support cases in which individual courts had ordered that a defence lawyer not disclose specific information to his or her client, such as the identity of an informer, the addresses of witnesses or the fact that the accused was being investigated for jury tampering. Judge Sands also rejected the accused’s argument that he had a right to be present at the CIPA hearing on the basis that such hearings revolved around questions of law and it was not essential for the accused to be present.⁵⁷⁸

One recent study has recommended that Congress amend CIPA to provide an independent process that would allow defence lawyers to be security-cleared in advance of particular cases and provide a fair means to allow the defence counsel to apply to the court for permission to consult with the accused about the classified information.⁵⁷⁹ That said, security clearances for lawyers and orders that they not share classified information with their clients only addressed the disclosure phase of the trial. In the United States, as in Canada, the accused would be present when evidence was presented against them in a criminal court.⁵⁸⁰ A former deputy counsel of the Central Intelligence Agency, Fred Manget, has recently recommended expanding CIPA “to allow nonpublic trial, protective secrecy orders that applied to jury members, criminal sanctions for unauthorized disclosure of classified information introduced in evidence and other means of confining national security information to the fewest necessary participants in a trial process.”⁵⁸¹ Many of these proposals would be available in Canada although exclusion of the public and the media would have to be justified under the Charter.

⁵⁷⁶ *United States v. Bin Laden* 2001 U.S. Dist. Lexis 719.

⁵⁷⁷ *Ibid* at para 15.

⁵⁷⁸ *Ibid* at para 22.

⁵⁷⁹ Serrin Turner and Stephen Schulhofer *The Secrecy Problem in Terrorism Trials* (New York: Brennan Center, 2005) at 80.

⁵⁸⁰ Robert Chesney “The American Experience with Terrorism Prosecutions” in vol. 3 of the *Research Studies*

⁵⁸¹ Fred Manget “Intelligence and the Criminal Law System” (2006) 17 *Stanford Law and Policy Rev.* 415 at 428.

4. Notice Provisions

The requirement for notice of an intent to introduce classified information under s.5 of CIPA, as well as the requirements for *in camera* hearings to determine whether the information should be disclosed or whether some form of substitution could be used, have been upheld in the United States in the face of repeated constitutional attack. Courts have generally held that the notice provisions do not violate the accused's right against self-incrimination because they do not require an accused to reveal all of his defence, plans for cross-examination or plans to testify, but only an intent to use classified information.⁵⁸² The two-court structure of s.38 of the CEA, along with the ability of the accused to make *ex parte* submissions to the Federal Court judge, as well as the ability to segregate the prosecutors at trial from the prosecutors at the s.38 proceedings, may provide more protections in Canada than in the United States for the accused's interest in not prematurely disclosing the defence than the American CIPA procedures.

5. Means of Reconciling Secrecy with Disclosure

CIPA is designed to give both governments and judges the greatest flexibility possible in reconciling the state's interests in the secrecy of security intelligence with the interests of the accused and the public in the disclosure of evidence. CIPA allows the government to propose substitutions, admissions and summaries for classified information at two different junctures. Section 4 of CIPA allows the United States to propose a summary, admission or substitution on an *ex parte* basis. This section has been strongly criticized as forcing the court to decide the adequacy of the substitution or summary at an early stage of the proceedings and without the benefit of the accused's argument or knowledge of the accused's defence. It is an explicit statutory displacement of a strong presumption against *ex parte* hearings even in the national security context. For example the United States Supreme Court has warned in the context of national security claims that "in our adversary system,

⁵⁸² See for example *United States v. Wen Ho Lee* 90 F.Supp. 1324. The defence lawyers in that case later wrote: "At the CIPA section 6 hearing, the defendant must establish the relevance of each listed item of classified information. This affords the prosecution a unique insight into the defence strategy, as defence counsel sets forth the theory of the defence and ties particular pieces of evidence to the theory. In no other part of the criminal justice system must the defendant provide such a complete explanation of the defence before trial without a reciprocal obligation on the prosecution. As with other aspects of CIPA, however, courts have found no constitutional defect in Section 6 procedures." John D. Cline and K.C. Maxwell "Criminal Prosecutions and Classified Information" Los Angeles Lawyer September, 2006 35 at 39.

it is enough for judges to judge. The determinations of what may be useful to the defence can properly and effectively be made only by an advocate.”⁵⁸³

Section 4 also does not provide statutory criteria for deciding the adequacy of the substitution, but it does provide that the government’s *ex parte* submissions should be preserved under seal and available to an appeal court. Even those who support the *ex parte* nature of the section 4 process suggest that “the court should retain the power to revoke any of its findings of adequacy of substitutions if it later finds that the defendant’s need for non-disclosed material outweighs the government’s interest in protecting the material.”⁵⁸⁴ As will be seen, the ability of trial judges to revisit their initial non or partial disclosure orders are similarly an important feature of both the Australian and British systems.

Section 6 of CIPA provides a second, less problematic, vehicle for substitutions and summaries. It only contemplates mandatory *ex parte* hearings with respect to the Attorney General’s certification that the disclosure of the information would cause identifiable damage to national security.⁵⁸⁵ It provides that upon any determination by the court that disclosure is necessary, the United States may propose the substitution for such classified information “of a statement admitting relevant facts” that the information would provide or “a summary of the specific classified information.” Under this section, the Court is to allow the proposed substitution “if it finds that the statement or summary will provide the defendant with substantially the same ability to make his defence as would disclosure of the specific classified information.” One court has indicated that this provision “does not preclude presentation of the defendant’s story to the jury, it merely allows some restriction in the manner in which the story will be told.”⁵⁸⁶

Section 8 of CIPA allows the trial judge considerable flexibility, when admitting classified information as evidence, to edit the information to

⁵⁸³ *United States v. Dennis* 384 U.S. at 875. In another case, the Court similarly warned that “An apparently innocent phrase, a chance remark, a reference to what appears to be a neutral person or event, the identity of a caller or the individual on the other end of a telephone, or even the manner of speaking or using words may have special significance to one who knows the more intimate facts of the accused’s life. And yet that information may be wholly colorless and devoid of meaning to one less well acquainted with all relevant circumstances.” *Alderman v. United States* 394 U.S. at 183-185.

⁵⁸⁴ Richard Salgado “Government Secrets, Fair Trials and the Classified Information Procedures Act” (1988) 98 Yale L.J. 427 at 445.

⁵⁸⁵ CIPA s.6(c) (2)

⁵⁸⁶ *United States v. Collins* 603 F. Supp at 304.

minimize harm to national security. Section 8(b) allows the editing of classified documents and photographs to exclude classified information “unless the whole in fairness ought to be considered.” Section 8 (c) addresses the difficulties of testimony that may blend classified and unclassified evidence, a difficulty that has led to the use of edited transcripts of testimony being used in the *Ribic* case discussed above. It provides that once an objection is made to testimony that will reveal classified information, “the court shall take such suitable action to determine whether the response is admissible as will safeguard against the compromise of any classified information” including proffers by the prosecution and the accused concerning the testimony and any information they seek to elicit. As in *Ribic*, this procedure seems to contemplate the reduction of live testimony to writing so as to allow more efficient and effective editing of the information to protect national security.⁵⁸⁷

6. Remedies for Non-Disclosure

The court is also accorded flexibility in fashioning an appropriate remedy under CIPA for the consequence of determinations that information cannot be disclosed. Section 6 of CIPA provides that in lieu of dismissing an indictment, the trial court can fashion an appropriate remedy for a decision not to disclose classified information to the defence. These remedies include dismissing parts of the indictment or striking or precluding all or part of the testimony of a witness. This approach is consistent with the remedial flexibility accorded to trial judges under s.38.14 of the CEA.

7. Interlocutory Appeals

The trial judge’s selection of lesser remedies, as well as the judge’s determination that classified information can be disclosed, is subject under s.7 of CIPA to an interlocutory appeal by the government. As was seen in the *Ribic* and *Khawaja* cases, determinations by the Federal Court under s.38 can be subject to appeal to the Federal Court of Appeal. Such proceedings can delay the start of trials. Section 7 of CIPA provides that the Court of Appeal “shall hear argument on such appeal within four days

⁵⁸⁷ *United States v. Moussaoui* 382 F.3d 453, 480 (4th Cir., 2004). For arguments that the trial judge’s original proposal that live testimony be given by videotape would be a fairer reconciliation of the competing demands of fairness to the accused and the protection of secrecy see Turner and Schulhofer *The Secrecy Problem in Terrorism Trials* at 41.

of the adjournment of the trial” and “shall render its decision within four days of argument on appeal”, and may dispense with written briefs and reasons. Section 38 of the CEA imposes ten-day time-limits on bringing appeals, but does not itself provide for expedited appeals. The accused under CIPA is not bound by the Court of Appeal’s interlocutory ruling on an appeal from conviction. This suggests that the value of interlocutory appeals mainly resides with the prosecution, who may otherwise be in a position of having to disclose the material ordered by the trial court or dismiss. In Canada, the use of a s.38.13 certificate may provide the state with an option short of dismissal.

8. The Management of the Relation between Intelligence and Evidence and Tensions Between Intelligence Agencies and Prosecutors

CIPA contemplates ongoing accountability structures to monitor how the government itself manages the relation between intelligence and evidence. Section 12 requires the Attorney General to issue guidelines about whether to prosecute cases involving classified information, and the preparation of written reasons in cases in which prosecutions are not undertaken because of the possibility of revealing classified information. Section 13 requires reports by the Attorney General to the legislative intelligence committees of such decisions. This provides a potential feedback loop about the adverse law enforcement consequences of the protection of classified information. One of the main themes of this study has been that security intelligence agencies need to be aware of the evidentiary consequences of their counter-terrorism practices, including their information sharing practices with foreign agencies. There should be some feedback loop so that intelligence agencies and the government consider the consequences of secrecy claims. Such a feedback loop is contemplated in the American legislation and it could serve as a brake on overbroad claims of secrecy that frustrate terrorism prosecutions.

CIPA was amended in 2000 as part of an intelligence reform and appropriations bill to require briefings between senior justice and senior intelligence officials. Section 9A of CIPA now provides:

(a) Briefings Required.— The Assistant Attorney General for the Criminal Division and the appropriate United States attorney, or the designees of such officials, shall provide briefings to the senior agency official, or the designee of such official, with respect to any case involving classified

information that originated in the agency of such senior agency official.

(b) Timing of Briefings.— Briefings under subsection (a) with respect to a case shall occur—

(1) as soon as practicable after the Department of Justice and the United States attorney concerned determine that a prosecution or potential prosecution could result; and

(2) at such other times thereafter as are necessary to keep the senior agency official concerned fully and currently informed of the status of the prosecution.⁵⁸⁸

This provision can be seen as a legislative response to the tensions between the frequent desire of intelligence agencies to keep intelligence secret and the desire of prosecutors for evidence that can be disclosed and used in public trials. Mandated briefings could allow intelligence agencies to learn more about the disclosure and evidentiary demands of terrorism prosecutions, while also allowing prosecutors to learn more about why intelligence agencies require that intelligence as well as methods and sources remain secret. Although legislation alone cannot mandate co-operation or resolve these tensions in individual cases, it can provide a framework for resolving such conflicts and tensions. Overclassification of secrets can impede terrorism prosecutions. In one post-9/11 terrorism prosecution, the government decided to declassify intercepts three days before trials, and commentators have recommended that classification of relevant information be reviewed once a prosecution has been commenced.⁵⁸⁹ Once a prosecution has commenced, intelligence agencies should start a process of reclassifying relevant information about the case in order to respond to the problem of overclassification.⁵⁹⁰

CIPA is most relevant in cases where the accused might seek access to classified information that is of no or minimal relevance to the case. In cases where the evidence is very relevant, it is unlikely that courts will hold that the evidence cannot be disclosed to the accused or that they will be able to devise non-classified substitutions that treat the accused

⁵⁸⁸ as added Pub. L. 106–567, title VI, § 607, Dec. 27, 2000, 114 Stat. 2855.)

⁵⁸⁹ Turner and Schulhofer *The Secrecy Problem in Terrorism Trials* at 27, 80.

⁵⁹⁰ *Ibid.*

fairly.⁵⁹¹ In those cases, the prosecutor may be faced with the stark dilemma of whether to disclose or to dismiss.⁵⁹² As one former prosecutor has concluded:

CIPA has never been viewed as assuring that all national security issues could be resolved. Since the executive branch maintains control of prosecutorial decisions, it still must decide whether or not to pursue a prosecution once an adverse ruling is rendered....What CIPA does do...is to eliminate certain forms of graymail in which the alleged secrets are actually irrelevant to the defence. If the evidence is not peripheral, it is deemed material to the defence and disclosure is therefore necessary to ensure a fair trial. If the national secrets and the illicit conduct are actually one and the same, ultimately, the prosecution may be thwarted.⁵⁹³

CIPA, however, provides some accountability for decisions to sacrifice prosecutions for the public interest in keeping secrets by providing written reasons for not prosecuting and reports to Congressional intelligence committees. It also now provides for early prosecutorial briefings of intelligence agencies about the evidential implications of their security intelligence work.

9. Summary

Although CIPA has already influenced s.38 of the CEA in terms of early notification requirements and giving judges a flexible array of options in reconciling the interests in secrecy and disclosure through editing, summaries and substitutions, it still differs from s.38 in a number of respects. CIPA allows questions of national security confidentiality to be decided by the judge who tries terrorism offences. The trial judge is provided with appropriate facilities to ensure the secrecy of the classified

⁵⁹¹ Brian Tamanaha "A Critical Review of The Classified Information Procedures Act" (1986) 13 Am. J. Crim. L. 277 at 305-306.

⁵⁹² On this dilemma see Robert Chesney "The American Experience with Terrorism Prosecutions" in vol. 3 of the Research Studies

⁵⁹³ Sandra Jordan "Classified Information and Conflicts in Independent Counsel Prosecutions" (1991) 91 Columbia L.Rev. 1651 at 1662-1663.

information.⁵⁹⁴ CIPA contemplates that national security confidentiality issues will be factored-in to general case management questions, whereas s.38 of the CEA delegates these to a separate court. The trial judge under CIPA is able to revisit initial non-disclosure orders, whereas the trial judge in Canada must accept non or partial disclosure orders made by the Federal Court before trial, while retaining the ability to fashion a remedy for the accused to respond to any non-disclosure.

Another difference between CIPA and the CEA is that CIPA has been interpreted to allow the trial judge in appropriate cases to require defence lawyers to obtain security clearances as a condition of having access to classified information. This procedure has, however, been challenged as restricting the ability of the defence lawyer to reveal the classified information to his or her client. The defence lawyer can generally be expected to be in a better position to know the utility of the information to the defence than a separate lawyer such as a security-cleared special advocate or *amicus curiae*.

Finally, CIPA attempts to manage the inevitable tensions within government between the demands by intelligence agencies for secrecy and the interests of prosecutors in disclosure. It provides several potentially valuable feedback mechanisms so that the government, including legislative committees, is aware of the consequences of overbroad claims of either secrecy or overbroad demands for disclosure. Recommendations have been made that in order to respond to the problem of overclassification, intelligence agencies should reclassify information about a case once a prosecution has commenced.

B) United Kingdom

The United Kingdom, like the United States, allows trial judges to make and revisit determinations of national security confidentiality. The British experience is of particular note because of the role of statutory disclosure standards and security-cleared special advocates.

⁵⁹⁴ As one judge who conducted a post 9/11 terrorism prosecution has explained: "the court and the prosecution must ensure that [classified] information is maintained in a completely secure facility called a Secure Compartmented Information Facility (SCIF), which is basically a fully secured and alarmed office. All highly classified intelligence must not only be kept in a SCIF, but any review of this information- whether by the prosecutor, defence counsel, or the court must be done in the SCIF itself. I now have a SCIF near my chambers, and I can tell you that entering the SCIF and reviewing materials in it is something of a twilight-zone experience." Judge Gerald Rosen "The War on Terrorism in the Courts" (2004) 21 T.M. Cooley L.Rev. 159 at 164.

1. Disclosure Requirements

The disclosure regime used in a particular country may affect the need for recourse to obtain non-disclosure orders for reasons of national security confidentiality. The disclosure regime in the United Kingdom is quite complex. There is a common law regime of disclosure that governs disclosure in relation to offences in which the investigation began prior to April, 1997. The landmark case involved a wrongful conviction in a terrorism case. It articulated a broad right of disclosure of all relevant evidence somewhat similar to the *Stinchcombe* decision examined above.⁵⁹⁵ The *Criminal Procedure and Investigations Act 1996* narrowed this common law test by providing under s.3(1)(a) that primary disclosure must be made of any prosecution material which might undermine the case for the prosecution against the accused.⁵⁹⁶ Secondary disclosure under section 7(2)(a) was required for previously undisclosed material which might be reasonably expected to assist the accused's defence. Section 32 of the *Criminal Justice Act 2003* amended section 3(1)(a) of the 1996 Act to require primary disclosure of any previously undisclosed material "which might reasonably be considered capable of undermining the case for the prosecution against the accused or of assisting the case for the accused". As the House of Lords recently recognized:

⁵⁹⁵ In *R v Ward* [1993] 1 WLR 619, 674, the Court stated: "An incident of a defendant's right to a fair trial is a right to timely disclosure by the prosecution of all material matters which affect the scientific case relied on by the prosecution, that is, whether such matters strengthen or weaken the prosecution case or assist the defence case. This duty exists whether or not a specific request for disclosure of details of scientific evidence is made by the defence. Moreover, this duty is continuous: it applies not only in the pre-trial period but also throughout the trial". See also *R v Keane* [1994] 1 WLR 746, 752 in which the Court held that the prosecution should put before the judge only those documents which it regarded as material but wished to withhold on grounds of public interest immunity. "Material" evidence was defined as evidence which could be seen, "on a sensible appraisal by the prosecution: (1) to be relevant or possibly relevant to an issue in the case; (2) to raise or possibly raise a new issue whose existence is not apparent from the evidence which the prosecution proposes to use; (3) to hold out a real (as opposed to fanciful) prospect of providing a lead on evidence which goes to (1) or (2)".

⁵⁹⁶ A 2006 Protocol for the Control and Management of Unused Material in the Crown Court issued by the Court provides detailed guidance for the disclosure process that supplements the statutory guidance. It provides: "the more complex the case, the more important it is for the prosecution to adhere to the overarching principle in paragraph 54 and ensure that sufficient prosecution resources are allocated to the task. Handing the defence the 'keys to the warehouse' has been the cause of many gross abuses in the past, resulting in huge sums being run up by the defence without any proportionate benefit to the course of justice. These abuses must end. The public rightly expects that the delays and failures which have been present in some cases in the past where there has been scant adherence to sound disclosure principles will be eradicated by observation of this Protocol. The new regime under the Criminal Justice Act and the Criminal Procedure Rules gives judges the power to change the culture in which such cases are tried. It is now the duty of every judge actively to manage disclosure issues in every case. The judge must seize the initiative and drive the case along towards an efficient, effective and timely resolution...In this way the interests of justice will be better served and public confidence in the criminal justice system will be increased." at <http://www.hmcourts-service.gov.uk/publications/guidance/disclosure.htm>

Whether in its amended or unamended form, section 3 does not require disclosure of material which is either neutral in its effect or which is adverse to the defendant, whether because it strengthens the prosecution or weakens the defence.⁵⁹⁷

In general, disclosure obligations in both the United States⁵⁹⁸ and the United Kingdom are less broad than in Canada. Both the United States and the United Kingdom attempt to flesh-out disclosure requirements in statutes and other rules⁵⁹⁹ while, as discussed above, Canada relies on a case-by-case adjudication under the Charter. Both the decreased breadth and increased certainty of disclosure requirements in the United States and the United Kingdom may make it less necessary for prosecutors to claim national security confidentiality over material that may be relevant to a case, but which does not significantly weaken the prosecution's case or strengthen the accused's case.

2. Public Interest Immunity

In a 1993 case which overturned a terrorism conviction in part because the Crown had not made full disclosure, the Court of Appeal criticized the prosecution for acting "as a judge in their own cause on the issue of public interest immunity". The Court of Appeal indicated that if the Crown was "not prepared to have the issue of public interest immunity determined by the court, the result must inevitably be that the prosecution will have to be abandoned."⁶⁰⁰ In some ways, this sounds a similar warning to that articulated in *Khela* about prosecutors taking issues of disclosure into their own hands. At the same time, more recent disclosure developments in the United Kingdom have stressed the importance of the prosecutor not simply dumping all possibly relevant information on the accused, but rather only disclosing information that is required under statutory disclosure requirements.

The Court of Appeal decided that while the material over which public interest immunity is claimed must always be disclosed to the court, and such applications should generally be disclosed to the defence, there may be cases in which the general category of the evidence claimed to

⁵⁹⁷ *R. v. H and C* [2004] UKHL 3 at para 17.

⁵⁹⁸ *Brady v. Maryland* 373 U.S. 83.

⁵⁹⁹ See Rule 16 of the Federal Rules of Criminal Procedure

⁶⁰⁰ *R. v. Ward* [1993] 1 W.L.R. 619 at 648.

be covered could not be disclosed to the accused because it would reveal secrets. The Court of Appeal indicated that there may be exceptional cases in which no notice at all would be given to the accused because such notice would reveal the nature of the evidence in question.⁶⁰¹ In Canada, s.38.04(5) of the CEA vests in the Federal Court a judicial discretion to give notice of a hearing and to make representations, but s.38.08 contemplates an automatic review by the Federal Court of Appeal in cases where a judge determines that party's interest is adversely affected, but that party has not been allowed to make representations to the judge.

In 1994, the Court of Appeal stressed that the Crown need only apply for public interest immunity with respect to material evidence that would be subject to a duty of disclosure. It warned against prosecutors dumping "all its unused material in the court's lap to sort through it regardless of its materiality to the issue present or potential." It also warned that "the more full and specific the indication the defendant's lawyers give of the defence or issues they are likely to raise, the more accurately both prosecution and judge will be able to assess the value to the defence of the material."⁶⁰² As discussed above, the judge conducting s.38 hearings in the *Khawaja* prosecution has expressed some concern both that the Crown has sought non-disclosure orders for administrative matters and general analytical intelligence that is not relevant to the case or could not be of any assistance to the accused. The Court has also expressed concerns that the accused had not taken the opportunity even on an *ex parte* basis to inform the judge about the accused's defences. Prosecutors can be criticized if they define their disclosure obligations either too broadly or too narrowly. In borderline cases, it may be advisable for the prosecutor to be able to seek guidance from the trial judge about whether sensitive information is even subject to disclosure obligations.

The House of Lords considered the proper procedures and approaches to public interest immunity in *R. v. H. and C*⁶⁰³. It recognized the close connections between disclosure and public interest immunity when it stressed that there would be no need to claim immunity for material that was not subject to disclosure "if material does not weaken the prosecution case or strengthen that of the defendant, there is no requirement to disclose it." It also warned about the dangers of the accused being "permitted to make general and unspecified allegations and then seek

⁶⁰¹ *R. v. Davis, Johnson and Rowe* [1993] 1 W.L.R. 613

⁶⁰² *R. v. Keane* [1994] 1 W.L.R. 746 at 752

⁶⁰³ [2004] UKHL 3

far-reaching disclosure in the hope that material may turn up to make them good. Neutral material or material damaging to the defendant need not be disclosed and should not be brought to the attention of the court.”⁶⁰⁴ An approach to disclosure that is more restrictive than in Canada -- especially in relation to material in state files that is damaging to the accused but will not be used as evidence -- limits the opportunities in which the Crown must make non-disclosure applications in order to protect secrets.

The House of Lords has outlined the following approach which seeks to exclude from a public interest immunity application any material that the Crown need not disclose, and material that would not cause serious prejudice to an important public interest:

- (1) What is the material which the prosecution seek to withhold? This must be considered by the court in detail.
- (2) Is the material such as may weaken the prosecution case or strengthen that of the defence? If No, disclosure should not be ordered. If Yes, full disclosure should (subject to (3), (4) and (5) below) be ordered.
- (3) Is there a real risk of serious prejudice to an important public interest (and, if so, what) if full disclosure of the material is ordered? If No, full disclosure should be ordered.
- (4) If the answer to (2) and (3) is Yes, can the defendant's interest be protected without disclosure or disclosure be ordered to an extent or in a way which will give adequate protection to the public interest in question and also afford adequate protection to the interests of the defence? ...
- (5) Do the measures proposed in answer to (4) represent the minimum derogation necessary to protect the public interest in question? If No, the court should order such greater disclosure as will represent the minimum derogation from the golden rule of full disclosure.
- (6) If limited disclosure is ordered pursuant to (4) or (5), may the effect be to render the trial process, viewed as a whole, unfair to the defendant? If Yes, then fuller disclosure

⁶⁰⁴ bid at para 35

should be ordered even if this leads or may lead the prosecution to discontinue the proceedings so as to avoid having to make disclosure.

(7) If the answer to (6) when first given is No, does that remain the correct answer as the trial unfolds, evidence is adduced and the defence advanced?⁶⁰⁵

In cases where the material is both subject to the duty of disclosure because it would weaken the prosecution or strengthen the defence and there is a serious prejudice to an important public interest, the House of Lords stressed means to reconcile the demands of secrecy and disclosure through devices such as court-approved editing or summarizing the evidence, or having the prosecution make admissions of facts. This flexible approach is consistent with the orientation of both the American CIPA legislation and s.38.06 of the CEA.

There are two features of the British approach to public interest immunity which are somewhat unique and merit consideration.⁶⁰⁶ The first is the recognition by the House of Lords that: "in appropriate cases the appointment of special counsel may be a necessary step to ensure that the contentions of the prosecution are tested and the interests of the defendant protected... In cases of exceptional difficulty the court may require the appointment of special counsel to ensure a correct answer to questions (2) and (3) as well as (4)." The House of Lords recognized that the appointment of special counsel was not without difficulties. These problems included the lack of explicit authorizing legislation, the delay caused while the special advocate becomes familiar with a complex case and "ethical problems, since a lawyer who cannot take full instructions from his client, nor report to his client, who is not responsible to his client and whose relationship with the client lacks the quality of confidence inherent in any ordinary lawyer-client relationship, is acting in a way hitherto unknown to the legal profession."⁶⁰⁷ The Federal Court Trial Division's recent decisions that have contemplated or appointed security

⁶⁰⁵ *ibid* at para 36.

⁶⁰⁶ The 2001 report of the Auld Committee recommended introduction of a scheme for instruction by the court of special independent counsel to represent the interests of the defendant in those cases at first instance and on appeal where the court now considers prosecution applications in the absence of the defence in respect of the non-disclosure of sensitive material." *The Review of the Criminal Courts in England and Wales* (2001) at para 197.

⁶⁰⁷ *R v. H and C* [2004] UKHL 3 at para 22.

cleared counsel in s.38 proceedings⁶⁰⁸ have not discussed the practical or ethical problems identified by the House of Lords.

The second important feature of the British approach is the emphasis that it places on the continuing review of any non-disclosure order made by the trial judge. In other words, any such order “should not be treated as a final, once-and-for-all, answer but as a provisional answer which the court must keep under review.”⁶⁰⁹ This was underlined by its recognition that a special advocate if appointed would likely have “to assist the court in its continuing duty to review disclosure.”⁶¹⁰ In contrast, the Canadian procedure requires the Federal Court judge to reach a final decision under s.38. Although this decision may be subject to clarification by that judge or to appeal to the Federal Court of Appeal, it must at the end of the day be accepted by the trial judge.

The above procedure should also be considered in light of the European Court of Human Rights Grand Chamber’s decision in *Edwards and Lewis v. the United Kingdom*⁶¹¹ which held that the right to a fair trial had been violated in public interest immunity proceedings. The Grand Chamber endorsed the following consideration of the law on disclosure by the Fourth Chamber:

It is in any event a fundamental aspect of the right to a fair trial that criminal proceedings, including the elements of such proceedings which relate to procedure, should be adversarial and that there should be equality of arms between the prosecution and defence. The right to an adversarial trial means, in a criminal case, that both prosecution and defence must be given the opportunity to have knowledge of and comment on the observations filed and the evidence adduced by the other party (ibid., § 51). In addition, Article 6 § 1 requires that the prosecution authorities should disclose to the defence all material evidence in their possession for or against the accused (ibid.)

The entitlement to disclosure of relevant evidence is not, however, an absolute right. In any criminal proceedings

⁶⁰⁸ *Canada v. Khawaja* 2007 FC 463 aff’d without reference to the ability to appoint security cleared counsel 2007 FCA 388; *Khadir v. The Attorney General of Canada* 2008 FC 46; *Canada (Attorney General) v. Khawaja* 2008 F.C. 560.

⁶⁰⁹ *R v. H and C* supra at para 36.

⁶¹⁰ ibid at para 22.

⁶¹¹ Judgment of October 27, 2004

there may be competing interests, such as national security or the need to protect witnesses at risk of reprisals or keep secret police methods of investigation of crime, which must be weighed against the rights of the accused. In some cases it may be necessary to withhold certain evidence from the defence so as to preserve the fundamental rights of another individual or to safeguard an important public interest. Nonetheless, only such measures restricting the rights of the defence which are strictly necessary are permissible under Article 6 § 1. Furthermore, in order to ensure that the accused receives a fair trial, any difficulties caused to the defence by a limitation on its rights must be sufficiently counterbalanced by the procedures followed by the judicial authorities (ibid, § 52)....⁶¹²

These statements suggest a willingness to accept limits on the right of disclosure for reasons of national security provided that they are “sufficiently counterbalanced” by other procedures to ensure a fair trial. Some commentators have suggested that the Grand Chamber’s emphasis in *Edwards and Lewis* on the importance of adversarial challenge suggests that special advocates should be used in public interest immunity proceedings.⁶¹³

On the facts of the *Edwards and Lewis* cases, which involved public interest immunity applications that shielded investigative techniques used by the police in cases in which the accused claimed entrapment defences, the Grand Chamber held that the right to a fair trial in Article 6 had been violated and endorsed the following conclusion:

In the present case, however, it appears that the undisclosed evidence related, or may have related, to an issue of fact decided by the trial judge. Each applicant complained that he had been entrapped into committing the offence by one or more undercover police officers or informers, and asked the trial judge to consider whether prosecution evidence should be excluded for that reason. In order to conclude whether or not the accused had indeed been the victim of improper incitement by the

⁶¹² ibid at para 46.

⁶¹³ Mike Redmayne “Criminal Justice Act 2003: Disclosure and its Discontents” [2004] Crim L.Rev. 441 at 456-457 (in reference to the lower chamber’s ruling in *Edwards and Lewis v. The United Kingdom*)

police, it was necessary for the trial judge to examine a number of factors, including the reason for the police operation, the nature and extent of police participation in the crime and the nature of any inducement or pressure applied by the police ... Had the defence been able to persuade the judge that the police had acted improperly, the prosecution would, in effect, have had to be discontinued. The applications in question were, therefore, of determinative importance to the applicants' trials, and the public interest immunity evidence may have related to facts connected with those applications. Despite this, the applicants were denied access to the evidence. It was not, therefore, possible for the defence representatives to argue the case on entrapment in full before the judge. Moreover, in each case the judge, who subsequently rejected the defence submissions on entrapment, had already seen prosecution evidence which may have been relevant to the issue...

In these circumstances, the Court does not consider that the procedure employed to determine the issues of disclosure of evidence and entrapment complied with the requirements to provide adversarial proceedings and equality of arms or incorporated adequate safeguards to protect the interests of the accused. It follows that there has been a violation of Article 6 § 1 of the Convention in this case.⁶¹⁴

This ruling affirms that the fairness of non-disclosure depends on the relation between the non-disclosed information and the issues raised in the trial. In this case, the Grand Chamber was concerned that the non-disclosed information related to the entrapment defences raised by the accused.

In another public interest immunity case, the European Court of Human Rights found a violation of the right to a fair trial where the prosecutor's late disclosure of the material meant that it had only been reviewed by the Court of Appeal in *ex parte* proceedings, but not by the trial judge. The Court concluded:

⁶¹⁴ Judgment of October 27, 2004 at para 46.

The Court does not consider that this procedure before the appeal court was sufficient to remedy the unfairness caused at the trial by the absence of any scrutiny of the withheld information by the trial judge. Unlike the latter, who saw the witnesses give the testimony and was fully versed in all the evidence and issues in the case, the judges in the Court of Appeal were dependent for their understanding of the possible relevance of the undisclosed material on transcripts of the Crown Court hearings and on the account of the issues given to them by prosecuting counsel. In addition, the first instance judge would have been in a position to monitor the need for disclosure throughout the trial, assessing the importance of the undisclosed evidence at a stage when new issues were emerging, when it might have been possible through cross-examination seriously to undermine the credibility of key witnesses and when the defence case was still open to take a number of different directions or emphases.⁶¹⁵

This case is relevant to the Canadian experience because it suggests that the European Court of Human Rights is uneasy about the fairness of procedures that do not allow the trial judge to revisit non-disclosure issues in light of the defence case and the cross-examination of witnesses at trial.

The British experience is instructive in Canada in several respects. It indicates that questions of public interest immunity cannot be divorced from the scope of disclosure obligations. Britain has moved away from relying on court decisions to define the prosecutor's disclosure obligations and legislation has both reduced disclosure obligations and made them more certain. The British example also provides some experience with the use of special advocates in public interest immunity proceedings. It warns of the danger of increased delay and of the difficulty of the special

⁶¹⁵ *Rowe and Davis v. United Kingdom* (2000) 30 E.H.R.R. 1 at para 65. See also *Atlan v. The United Kingdom* (2001) E.H.R.R. 33 to the same effect. One commentator has observed that these cases illustrate "the importance of entrusting the decision on PII to the trial judge because only he can shape proceedings to ensure that withholding the information does not result in unfairness to the defence. In England, whenever an application for PII is granted, it is the duty of the trial judge to keep the matter under review and, if events at the trial dictate, he must order that the interests of justice require disclosure of the relevant information after all. This appears to be the inevitable and sensible result of entrusting the original decision to the trial judge." Peter Duff "Disclosure of Evidence and Public Interest Immunity" (2008) *Scots Law Times* 63 at 66.

advocate to take meaningful instructions from the accused after the special advocate has seen the secret and undisclosed information.

Finally and most importantly, both the House of Lords and the European Court of Human Rights have placed considerable emphasis on the ability of the trial judge to revisit initial decisions that the disclosure of sensitive information is not required in light of an evolving trial, including the defence's case and defence cross-examination of witnesses. Although the courts have approached the trial judge's ability to revisit public interest immunity decisions mainly from the perspective of ensuring fairness to the accused, it also has an efficiency dimension because it allows the trial judge to include such issues in general case management issues. The trial judge can examine the undisclosed material and order non-disclosure, but be confident that he or she can revisit that order on his or her own motion as the trial evolves in order to ensure a fair trial. This approach is not an option under the two-court structure of s.38 of the CEA.

C) Australia

Australia has extensive recent experience with claims of national security confidentiality. Its Law Reform Commission has prepared an excellent report on the subject and it enacted new legislation to govern national security confidentiality in 2004. This new legislation has already been tested in completed terrorism prosecutions. In what follows, I will outline the history of public interest immunity claims in Australian, assess the major features of the new legislation and conclude with a case study in which the legislation was challenged and employed in a creative manner.

1. Public Interest Immunity Cases

A 1984 case dealt with a public interest immunity claim made to secure non-disclosure of the Australian Security Intelligence Organization's (ASIO) files about an informer in a case where a number of accused found with explosives were charged with conspiracy to commit murder and attempted murder. There were also possible connections between the case and a 1978 terrorist bombing aimed at an Indian delegation staying at the Hilton Hotel in Sydney. The trial judge accepted the Attorney General's claim of public interest immunity on the basis that his affidavit "asserts matters which this court should without more accept." The High Court in a 3:2 decision reversed this decision. Gibbs C.J. for the majority

distinguished the deferential approach that judges at the time took to public interest immunity applications in civil cases with the approach that should be applied to criminal cases. He stated that trial judges must attach:

...special weight to the fact that the documents may support the defence of an accused person in criminal proceedings. Although a mere “fishing” expedition can never be allowed, it may be enough that it appears to be “on the cards” that the documents will materially assist the defence. If, for example, it were known that an important witness for the Crown had given a report on the case to ASIO it would not be right to refuse disclosure simply because there were no grounds for thinking that the report could assist the accused. To refuse discovery only for that reason would leave the accused with a legitimate sense of grievance, since he would not be able to test the evidence of the witness by comparing it with the report, and would be likely to give rise to the reproach that justice had not been seen to be done.⁶¹⁶

Similar views about the importance of full disclosure in criminal cases were also expressed by Murphy J. who stated:

...the trial judge should have inspected the documents subpoenaed to ascertain if they contained anything which tended to show that the case against the accused was fabricated (or otherwise tended to assist the accused in their defence, either directly, for example, by providing a basis for cross-examination, or indirectly, by pointing to the existence of other material which might assist). There is a public interest in certain official information remaining secret; but there is also public interest in the proper administration of criminal justice. The processes of criminal justice should not be distorted to prevent an accused from defending himself or herself properly. If the public interest demands that material capable of assisting an accused be withheld, then the proper course may

⁶¹⁶ *Alister v. The Queen* (1984) 154 C.L. R. 404 at 415.

be to abandon the prosecution or for the court to stay proceedings.⁶¹⁷

Brennan J. wrote a third concurring judgment that warned of the dangers of disclosing too much intelligence to the accused. In his view, ASIO documents should only be admitted as evidence in relatively narrow circumstances related to the accused's innocence.⁶¹⁸

Wilson and Dawson J. dissented on the basis that "we do not think that the trial judge or this Court is in a position to do other than accept that disclosure of the information would endanger national security". They would have required the accused to demonstrate that the ASIO intelligence "would go substantially to proof of their innocence of the charges against them" before engaging in any balancing of the competing public interests for and against disclosure.⁶¹⁹

In light of these judgments, the Attorney General produced the ASIO files to the High Court. Gibbs C.J. concluded for four judges that the material should not have been disclosed and would not have affected the result in the trial. The High Court made this decision without hearing from the accused, noting that "it is the inevitable result when privilege is rightly claimed on grounds of national security."⁶²⁰ Gibbs C.J. concluded:

We have formed the clear view that none of the documents is relevant to the issues at the trial or could have been used for the purpose of cross-examining the Crown witnesses. When we say that, we do not discount the significance of the argument that the parties may be more able than the members of the court to discern the possible relevance of material in a trial of this kind, but we remain satisfied that the material would not assist the appellants... We are further satisfied that the appellants have not lost the chance of an acquittal by the failure to produce the material.⁶²¹

617 Ibid at 431

618 Ibid at 455

619 Ibid at 439

620 Ibid at 469

621 Ibid at 469

The majority's judgment supports the importance of having judges examine intelligence files in criminal cases, as well as the conclusion that such intelligence may often not assist the defence.

Murphy J. dissented on the basis that after examining the ASIO documents he had a doubt about their relevance to the outcome of the case. In his view, the High Court should have heard argument from the accused about the possible relevance of the undisclosed intelligence. He stated that he had "no objection to disclosure of the documents to counsel for the parties upon appropriate undertakings being given."⁶²² Murphy J. concluded in strong language:

If the defence, or both parties, could assist the Court to a conclusion that the material would have been of assistance to the defence, it is a grave injustice to preclude them from doing so. If, however, the documents would not have assisted the defence, then it would be more satisfactory and more just if such a conclusion were to be reached after having the assistance of both parties. In my opinion, it is an injustice to both the Crown and the accused and casts a further shadow over this case that the Court makes a decision without the proffered assistance of both prosecution and defence. I find it a strange and disturbing case. I adhere to the view which I expressed in the first disposition of special leave to appeal, that in all cases there has been a substantial miscarriage of justice and that the appeal should be granted and the convictions set aside.⁶²³

This dissenting judgment stands for the proposition that decisions about disclosure will be improved by participation by the accused with "appropriate undertakings". The accused was subsequently convicted. They were, however, later pardoned on the basis that the convictions were unsafe.

A second case that led Australia to re-examine the relation between intelligence and evidence was a 2001 prosecution of a government employee named Lappas who was charged with offences relating to the disclosure of classified information to a foreign power. The

⁶²² Ibid at 470

⁶²³ Ibid at 470

government claimed public interest immunity with respect to two of the documents in the middle of a criminal trial. The trial judge noted that it was regrettable that the claim was made “at this late stage” because it would have been possible for the prosecution to have charged the accused with a different offence, one which would not require proof that the classified information would be of use to a foreign power, an element of the offence that “puts directly at issue the contents of the document”⁶²⁴. The government proposed to introduce a redacted shell of the document to be supplemented by some general oral evidence about the content of the document. The trial judge resisted such a procedure on the basis that “there could be no cross-examination on whether the interpretation [offered in oral evidence] accurately reflected the contents for that would expose the contents. Nor could a person seeking to challenge the interpretation give their own oral evidence of the contents for that also would expose those contents. The whole process is redolent with unfairness....I do not accept that upholding the claim with the exceptions expressed to it would enable justice to be done to either the prosecution or the defence case. More particularly, I do not think the accused can have a fair trial unless far more of the text of the documents is disclosed to enable the accused, if he wishes to do so, to give evidence concerning it.”⁶²⁵ In the result, the trial judge stayed the relevant counts of the indictment, although the accused was convicted on other counts that did not involve the document. This case confirms how reluctance to disclose some classified material may undermine a prosecution, but also that the particular nature of the criminal charge may affect how much secret material is relevant and must be disclosed to the accused.

The *Lappas* case, like the *Ribic* case, raised the issue of whether adequate provisions had been made in Australian law for early notice and resolution of national security confidentiality issues and for a flexible approach that would provide workable and fair alternatives to the extremes of disclosing or not disclosing the materials.

2. The Australian Law Reform Commission's Report

In 2004, the Australian Law Reform Commission produced an extensive final report on secrecy in a variety of proceedings. It recommended that all parties be required to give notice to the court and other parties as soon

⁶²⁴ *R. v. Lappas and Dowling* [2001] ACTSC 115 at para 20

⁶²⁵ *R. v. Lappas and Dowling* [2001] ACTSC 115 at para 14.

as practicable about whether classified or sensitive information would be used. The Attorney General of Australia would have to be notified and would be able to intervene in criminal cases that were prosecuted by other officials. The court would have extensive powers to conduct pre-trial hearings and make directions with respect to the relevance and admissibility of sensitive or classified information. The Commission specifically recommended that:

In criminal matters, the court may order that the prosecution be excused in part or whole from any obligation that it would otherwise have been under to disclose classified national security information or other national security information to an accused person, or that any such obligation be varied, subject to the following safeguards:

(a) the information in question is not central to the case before the court;

(b) the information must not be exculpatory of, or reasonably assist, the accused;

(c) the prosecution is precluded from relying on or adducing the information at trial;

(d) the application and the reasons for the court's order are made known to the accused...

This recommendation was subject to another recommendation that on application of any party or on its own motion, "the court or tribunal may order the disclosure of material that it had previously ordered could be withheld or introduced in another fashion in the light of subsequent developments in the proceedings or elsewhere which alter the requirements of justice in the case or reduce the sensitivity of the material in question."⁶²⁶ This latter power is similar to the ability of British courts to re-visit public interest immunity determinations. It recognizes that both the demands of secrecy and fairness may evolve during a trial. The report also addressed whether lawyers should be required to obtain security clearances as a precondition to obtaining access to sensitive or classified material. It noted that in the *Lappas* case discussed above,

⁶²⁶ Australian Law Reform Commission *Keeping Secrets The Protection of Classified and Security Sensitive Information* (2004) Recommendation 11-29.

the defence lawyer declined to seek a security clearance and the trial judge decided that there was no power to require a clearance. The accused's lawyer was, however, allowed to see the documents subject to a confidentiality undertaking that only allowed the material to be disclosed to other lawyers and the accused and to take appropriate steps for the secure storage and eventual destruction of the material.⁶²⁷ The Commission commented that:

A security clearance does not of itself guarantee that information is safe from improper disclosure. Indeed, it is not facetious to say that, when national security information has been disclosed unlawfully, it is usually at the hands of someone with a high-level security clearance—since by definition these are the people with access to such information. On the other hand, requiring a security clearance is an essential feature of sensible risk management in that it helps to prevent people who are discerned to be security risks from gaining access to the information, as well as providing training and reinforcement about proper handling of such sensitive information.⁶²⁸

The Commission recommended that on a motion of any party or its own motion, the Court may require that specified material only be disclosed to lawyers with security clearances. It stressed that this would reassure allies, allow lawyers to have access to information and not unduly restrict choice of counsel. For the Commission, "this issue is not primarily about the rights of lawyers but rather about the rights of clients to be assured that their lawyers have access to all information relevant to their case."⁶²⁹ It also recommended that the court have the same power to require specific undertakings of confidentiality. It concluded that security clearances and undertakings served distinct but complementary purposes, with the security clearance going to issues of character and reliability and undertakings relating to specific obligations in specific circumstances.⁶³⁰ Agreements between the accused and the Attorney General with respect to the disclosure of sensitive material were to be encouraged, including

⁶²⁷ *ibid* at 6.26. The Law Commission noted, however, that "these undertakings apparently did not satisfy the foreign power from which the two highly sensitive documents were sourced since it continued to refuse to permit them to be tendered in the proceedings." Appendix 3 at para 30.

⁶²⁸ *Ibid* at 6.95

⁶²⁹ *Ibid* at 6.98

⁶³⁰ *Ibid* at 6.97

the possibility of lower sentences to recognize the accused's co-operation in such matters.⁶³¹

The Law Commission's report, also dealt with the issue of admissibility of classified information in court and proposed that judges be allowed to use a variety of flexible and innovative procedures to reconcile national security interests with the need to disclose and admit relevant evidence. The devices that trial judges should be empowered to use would include:

- (i) the redaction, editing or obscuring of any part of a document containing or adverting to classified or sensitive national security information;
- (ii) replacing the classified or sensitive national security information with summaries, extracts or transcriptions of the evidence that a party seeks to use, or by a statement of facts, whether agreed by the parties or not;
- (iii) replacing the classified or sensitive national security information with evidence to similar effect obtained through unclassified means or sources;
- (iv) ... concealing the identity of any witness or person identified in, or whose identity might reasonably be inferred from, classified or sensitive national security information or from its use in court or tribunal proceedings (including oral evidence), and concealing the identity of any person (including jurors) who come into contact with classified or sensitive national security information;
- (v) the use of written questions and answers during otherwise oral evidence;
- (vi) closed-circuit television, computer monitors, headsets and other technical means during proceedings by which the contents of classified or sensitive national security information may be obscured from the public or other particular people;

⁶³¹ Ibid Recommendations 11-16.

(vii) restrictions on the people to whom any classified or sensitive national security information may be given or to whom access to that information may be given (which may include limiting access to certain material to people holding security clearances to a specified level);

(viii) restrictions on the extent to which any person who has access to any classified and sensitive national security information may use it; and

(ix) restrictions on the extent to which any person who has access to any classified and sensitive national security information (including any juror) may reproduce or repeat that information.⁶³²

With respect to the use of anonymous witnesses, the Court warned that the accused and his or her lawyers should generally be able to see the witness and the court should be reluctant to convict “either solely or to a decisive extent on the testimony of any anonymous witness.”⁶³³

Although the Commission was prepared to recommend a wide range of innovative means to reconcile the competing interests in secrecy and disclosure, it drew the line at the use of “secret evidence” in criminal cases that was not disclosed to the accused. It reasoned that:

As a matter of principle, the leading of secret evidence against an accused, for the purpose of protecting classified or security sensitive information in a criminal prosecution, should not be allowed. To sanction such a process would be in breach of the protections provided for in Article 14 of the International Covenant on Civil and Political Rights for an accused to be tried in his or her presence and to have the opportunity to examine, or have examined any adverse witnesses. Where such evidence is central to the indictment, to sanction such a process would breach basic principles of a fair trial, and could constitute an abuse of process.⁶³⁴

⁶³² Ibid Recommendation 11-10

⁶³³ Ibid Recommendation 11-11

⁶³⁴ Ibid at 11.203

The Commission also recommended that, in any case in which the judge “suppressed evidence which in the judge’s opinion must raise a reasonable doubt as to the guilt of the accused, the court may enter a verdict of acquittal or order that no further proceedings be brought for the crime(s) charged.”⁶³⁵ At the same time, the Commission recommended that *ex parte* procedures could be used with respect to obtaining orders that material need not be disclosed to the accused, and that public interest immunity applied to the material.⁶³⁶

The Commission also proposed that the Attorney General retain the right to issue a certificate prohibiting court-ordered disclosure, but that the court retain the right to stay any part of a proceeding as a result of the certificate.⁶³⁷ In some ways, this duplicates the checks and balances available in Canada with respect to the use of the Attorney General’s certificate under s.38.13 of the CEA and the ability of trial judges to stay proceedings under s.38.14 as a result of non-disclosure orders or certificates.

Finally, the Commission recognized that adequate handling of sensitive and classified material would require courts to take adequate precautions for keeping secrets. It recommended that the Attorney’s General department should train officers who would be answerable to their assigned court to assist federal and state courts on the “technical aspects of the physical storage and handling of classified or sensitive national security information.”⁶³⁸

3. The National Security Information Act

Even before the Australian Law Reform Commission had delivered its final report a comprehensive *National Security Information Act*⁶³⁹ was introduced in the Commonwealth Parliament. This bill followed many of the directions proposed by the Law Reform Commission, but departed from them in some respects. The Act has already been amended to include civil proceedings. My discussion will focus on the current version of the

⁶³⁵ Ibid Recommendation 11-26.

⁶³⁶ Ibid at 11.205

⁶³⁷ Ibid Recommendation 11-33.

⁶³⁸ Ibid Recommendation 11-38.

⁶³⁹ *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) s 24. For a critical overview of the act see Patrick Emerton ‘Paving the Way for Conviction without Evidence’ (2005) 4 *Queensland University of Technology Law and Justice Journal* 1.

act as it relates to disclosure and the relation between secret intelligence and public evidence in criminal trials.

In part because the trial judge is the ultimate decision-maker about national security confidentiality, the Australian law places greater emphasis on trial management than s.38 of the CEA. Under s.21 of the Act, either the prosecutor or the defence in federal criminal proceedings can apply to the court to hold a pre-trial conference in relation to the disclosure of national security information. The court under s.22 may make orders to give effect to agreements reached between the accused and the prosecutor. These provisions recognize the complexity of most trials involving intelligence and attempt to promote efficient pre-trial management.

As under s.38 of the CEA, both prosecutors and the accused have obligations to notify the Attorney General of Australia as soon as practicable if they know they will disclose or call a witness who will disclose national security information. The judge is then required to adjourn proceedings until the Attorney General decides whether to issue a certificate opposing the disclosure or one setting-out terms for the disclosure. In the case where an objection is raised during the examination of the witness, the trial judge is also required to adjourn hearings after having obtained the witness's written answer to the question *in camera*.⁶⁴⁰ Although judged necessary to protect national security, these mandatory adjournment requirements underline how such proceedings can slow the trial process.

After having received notice, the Attorney General has the option of authorizing the disclosure of the information with information deleted and a summary attached, or with a statement of the facts that the information would likely prove.⁶⁴¹ The Attorney General may also provide a certificate prohibiting the calling of a certain witness on national security grounds.⁶⁴² In this way, the Attorney General is given the "first crack" at reconciling the competing goals of secrecy and disclosure, and his or her decisions are considered binding and conclusive until reviewed by a court.⁶⁴³ The Act makes it an offence punishable by two years imprisonment to disclose material in a matter that is not contemplated in the Attorney's General certificate.⁶⁴⁴

⁶⁴⁰ Ibid s.24(4), 25(7).

⁶⁴¹ Ibid s.26

⁶⁴² Ibid s.28

⁶⁴³ Ibid s.27

⁶⁴⁴ The various offences are contained in ss.40-46 of the Act.

The Attorney's General certificate is reviewed by the trial judge in a closed hearing in which the court may exclude the accused and any lawyer representing the accused who has not been given the appropriate security clearance.⁶⁴⁵ Section 39 of the Act allows the Attorney General to serve notice on a defence lawyer that they must obtain an appropriate security clearance to gain access to national security information. The judge must adjourn proceedings to allow this to happen, and can inform the accused of the consequences of having a lawyer without a security clearance. The Law Reform Commission's proposals would have vested the power to trigger security clearances in the court and this part of the legislation has been criticized as giving the Attorney General too much power in the security clearance process.⁶⁴⁶

At a closed hearing to review the Attorney General's certificate about what can be disclosed, the judge has the ability to change the terms of disclosure set by the Attorney General. In making this decision, however, the judge is instructed under s.31(7) of the Act to consider both risk of prejudice to national security and adverse effects on the accused's right to a fair hearing, including the conduct of his or her defence. Section 31(8) provides that in making its decision, the Court must give greatest weight to the risk of prejudice to national security. National security is defined broadly under the Act to include not only national defence and international relations, but also law enforcement interests broadly defined to include various forms of information gathering.⁶⁴⁷ The statutory provision that the judge must give greater weight to risks to national security has been criticized as a significant departure from the test for public interest immunity articulated in 1984 by the High Court in the *Alister* case discussed above.⁶⁴⁸ A recently retired High Court judge has commented that the law "does not direct the court to make the order

⁶⁴⁵ Ibid s.29. The appropriateness of the security clearance is determined not by the judge but by the Secretary of the Attorney-General's department.

⁶⁴⁶ Patrick Emerton "Paving the Way for Conviction without Evidence: A Disturbing Trend in Australia's 'Anti-Terrorism' Laws" (2004) 4 *Queensland U. Tech L. and Justice J.* 1 at 20-21. Emerton argues that the provision that a lawyer with an appropriate security clearance cannot be excluded from the closed hearing to review the Attorney's General certificate "offers little protection to the accused's right to a fair trial. First, there is no obligation on the part of the Secretary of the Attorney-General's Department to grant a security clearance at the appropriate level. Second, the defendant's rights turn entirely upon the executive's conception of an 'appropriate level' of security clearance." Ibid at 28

⁶⁴⁷ *National Security Information Act* s. 8. Section 11 defines law enforcement interests as a) avoiding disruption to national and international efforts relating to law enforcement, criminal intelligence, criminal investigation, foreign intelligence and security intelligence; (b) protecting the technologies and methods used to collect, analyse, secure or otherwise deal with, criminal intelligence, foreign intelligence or security intelligence; (c) the protection and safety of informants and of persons associated with informants; (d) ensuring that intelligence and law enforcement agencies are not discouraged from giving information to a nation's government and government agencies.

⁶⁴⁸ Patrick Emerton "Paving the Way for Conviction without Evidence: A Disturbing Trend in Australia's 'Anti-Terrorism' Laws" (2004) 4 *Queensland U. Tech L. and Justice J.* 1 at 30.

which the Attorney General wants. But it goes as close to it as it thinks it can."⁶⁴⁹

The court's reasons to affirm or alter the Attorney's General certificate must be given to the prosecutor and the Attorney General. They can make submissions to the court about whether the reasons themselves disclose national security information. The court must adjourn proceedings at the request of any party pending appeal and the court's order does not take effect until the appeal period has expired.⁶⁵⁰

The decision made by the trial judge to affirm or alter the Attorney's General certificate is not necessarily final. Section 19(2) provides that "An order under section 31 does not prevent the court from later ordering that the federal criminal proceeding be stayed on a ground involving the same matter, including that an order made under section 31 would have a substantial adverse effect on a defendant's right to receive a fair hearing." As in Britain, the ability of the trial judge to re-visit matters as the trial evolves can be seen as both a safeguard for the accused, and as a means for the judge to authorize limited or no disclosure subject to a reappraisal as the evidence in the case is placed before the trial judge.

Summary

The *National Security Information Act* has been controversial and as will be seen, it was challenged as unconstitutional in the first terrorism prosecution in which it was invoked. Many of the criticisms of the Act have revolved around the Attorney's General power with respect to the initial editing of evidence, the primacy given in the statute to national security over fair trial concerns and the Attorney's General power to require security clearances for defence lawyers. On all these issues, the Law Reform Commission would have given the judiciary more power to make its own determinations of the appropriate means to reconcile secrecy with disclosure. The Australian law, like s.38, encourages flexibility in reconciling disclosure with secrecy, through the use of devices such as summaries. The Law Reform Commission would have provided an even broader menu of alternatives, including the ability of witnesses to give anonymous testimony, testimony by way of video or closed-circuit television and testimony by written questions and answers in a manner not dissimilar to that used in *Ribic*.

⁶⁴⁹ Michael McHugh 'Terrorism Legislation and the Constitution' (2006) 28 *Australian Bar Review* 117 at 131.

⁶⁵⁰ *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) ss. 24,32, 33, 34, 36.

The Australian law has a number of distinguishing features from the Canadian approach. It gives the trial judge the power to decide issues involving national security confidentiality. It allows for pre-trial conferences to manage the many problems arising from disclosure of national security information. It provides the opportunity for defence lawyers to obtain security clearances. Finally, it allows the trial judge to revisit issues of disclosure as the trial evolves. As will be seen, the Australian law has already been tested in one completed terrorism prosecution.

4. The Lodhi Case: The New Australian Law Tested in a Completed Prosecution

The *National Security Information Act* was invoked in federal criminal proceedings against Faheem Lodhi, who was charged with a range of offences related to preparation for acts of terrorism. In December, 2005, the trial judge, Whealy J., rejected a challenge that the *National Security Information Act* was unconstitutional on the grounds that it was inconsistent with the exercise of judicial power and the implied freedom of speech in relation to political matters. Whealy J. stressed that the Act did not infringe “in any fundamental way upon the ordinary process of the establishment of guilt or innocence by judge and jury. The onus of proof does not alter. The rules of evidence are not changed. The discretions as to the exclusion of evidence in the trial remain untouched. The traditional protections given to an accused person are not put aside by legislation.”⁶⁵¹

The judge retained the ability to decide whether evidence and the courtroom would be open to the public.⁶⁵²

Whealy J. noted that the legislation provided for mandatory adjournment to provide for notice to, and a certificate from, the Attorney General about the admissibility of sensitive information, and that these procedures clearly could entail a delay.⁶⁵³ Nevertheless, he held that the legislation did not infringe on the court’s ability to control its own process, including staying proceedings. Although offences for failing to notify the Attorney General of an intent to introduce sensitive information were in the judge’s view “novel”, and even “startling”⁶⁵⁴, they did not directly infringe

⁶⁵¹ *R. v. Lodhi* [2006] NSWSC 571 at para 85

⁶⁵² *ibid* at para 124

⁶⁵³ *R. v. Lodhi* [2006] NSWSC 571 at para 86.

⁶⁵⁴ *Ibid* at para 94

on the function of the court. The same was true for requirements that court staff and personnel have security clearances. He also concluded that the statutory exclusions of the accused and non-security-cleared lawyers from the s.31 hearings were not “materially different from the situation that arises traditionally where a public interest immunity claim is made.”⁶⁵⁵

Whealy J. also found that the statutory terms for the review of the Attorney’s General certificate, including the requirement in s.31(8) that the court give the greatest weight to the risk of prejudice to national security as opposed to fair trial considerations, were not inconsistent with the judicial function. The law still allowed the judge to balance the competing interests and to stay proceedings if a fair trial was impossible. It did not make the Attorney’s General certificate conclusive. This conclusion that the tilting of the balance towards national security did not deny the accused a fair trial or interfere with the judicial function has now been upheld by the New South Wales Court of Criminal Appeals.⁶⁵⁶

Whealy J. held that a special security-cleared counsel could be appointed to represent the accused in a s.31 hearing despite the fact that the Act did not specifically provide for such an officer. Although not able to share classified information with the accused, a special advocate would still be “a legal representative of the defendant” and, as such, entitled to attend a closed hearing to review the Attorney’s General certificate.⁶⁵⁷ He also relied on the fact that the Act did not affect the ability of a court to control the conduct of a federal criminal proceeding.⁶⁵⁸ In many ways, this decision is similar to that made by the Federal Court Division in *Khawaja*, which affirmed the ability of the Federal Court, on its own discretion, to appoint a security-cleared *amicus curiae*.⁶⁵⁹

A number of other pre-trial rulings made in this case are of significance to the relation between intelligence and evidence. One was a decision to close the court whenever evidence was presented that disclosed ASIO’s dealing with sources or its relationship with a foreign agency. In reaching this decision, Whealy J. considered both a public and a confidential affidavit by the head of ASIO detailing the dangers of revealing ASIO

⁶⁵⁵ Ibid at para 96

⁶⁵⁶ *R. v. Lodhi* [2007] NSWCCA 360.

⁶⁵⁷ *R. v. Lodhi* [2006] NSWSC 586 at para 28.

⁶⁵⁸ *National Security Information (Criminal and Civil Proceedings) Act 2004* s.19(1).

⁶⁵⁹ 2007 FC 463 aff’d without reference to the ability to appoint security cleared lawyers 2007 FCA 388.

targets, members and methods. The accused was given a copy of the confidential affidavit. The judge also ordered that a transcript of these closed hearings with redactions for national security information could be given to the media.⁶⁶⁰

Whealy J. also dealt with the competing considerations of fairness to the accused, the open court principle and concerns about national security when ASIO officers testified. In pre-trial proceedings, he ordered that a screen be used so that the accused could not identify ASIO officers when they testified in order to prevent "the real possibility of the compromise of intelligence operations in Sydney".⁶⁶¹ These orders were upheld with the Court of Appeal deciding that the trial judge had balanced the competing principles of open trials and fairness of the accused with the need to protect national security.⁶⁶²

Justice Whealy has, however, commented in an extrajudicial speech that the screening of the accused from ASIO officers "had a high capacity to implant prejudice in the minds of the jurors." On the consent of the parties, the ASIO officers were allowed to give testimony by means of closed circuit television at the trial as opposed to the use of screens. Monitors were available to all court participants including the accused. The accused's monitor, however, was not operational, but this fact was presumably kept from the jury because of the position of the monitor. The parties agreed to this procedure as one that was less prejudicial to the accused than the screens that were used in the pre-trial proceedings. Justice Whealy noted that: "The fact that orders of this kind were sought at all highlights the tremendous clash existing between the need to protect national security matters and the rights of an accused to a fair trial. The resolution of the conflict between these notions presents challenges of the highest order for a trial judge."⁶⁶³

In another pre-trial motion, Whealy J. upheld Lodhi's request for a subpoena to both the Australia Federal Police and ASIO for all warrants with respect to the investigation of the accused and an alleged co-conspirator. The judge stressed that "it is, "on the cards" that the material" was relevant,⁶⁶⁴ noting that even the failure of such warrants to discover

⁶⁶⁰ *R. v. Lodhi* [2006] NSWSC 596 at para 29

⁶⁶¹ *Ibid* at para 59.

⁶⁶² *R. v. Lodhi* [2006] NSWCCA 101 at para 31

⁶⁶³ Justice Whealy "Terrorism" prepared for a conference for Federal and Supreme Court Judges, Perth 2007.

⁶⁶⁴ *R. v. Lodhi* 2006 NSWSC 585 at para 16

incriminating evidence could be of assistance to the defence. He rejected the prosecutor's arguments that the accused could only speculate whether such warrants existed.⁶⁶⁵

In another pre-trial motion, Whealy J. ruled that a person in American custody and two American FBI officers could testify by way of video link.⁶⁶⁶ He held that juries can judge credibility through videos and that the accused would not be prejudiced in this regard. He also indicated that the presence of an independent observer could ensure that the prisoner in American custody gave testimony freely.⁶⁶⁷

In an interesting speech given after the completion of the trial, Justice Whealy reflected on the implications of the Lodhi case for future terrorism trials. He stated that "delay and disturbance to the trial process is perhaps the most significant potential problem created by the legislation". In the end, Justice Whealy concluded that the trial was able to reach verdict because "there was a considerable degree of co-operation between experienced counsel for the prosecution and the defence. It was plainly the desire of all parties to ensure that the trial proceeded as normally as possible." Similar comments have, of course, been made in relation to the Bagri and Malik trial. At the same time, it cannot be assumed that counsel in all terrorism prosecutions will genuinely want the case to go to verdict. Reforms, especially with respect to the abolition of pre-trial appeals, may be necessary in order to ensure that procedures used to determine national security confidentiality do not frustrate terrorism trials.

Justice Whealy concluded his extra-judicial speech with comments that are directly relevant to the evolving relation between intelligence and evidence. He stated:

To my mind prejudice, delay and secrecy are the principal problems confronting a trial judge in these matters. I have endeavoured to argue in this paper that appropriate directions to jurors should mitigate and diminish the problem of bias and prejudice. Secondly, that sensible co-operation between counsel, and the use of appropriate pre-trial procedures, should reduce the problem of delay significantly. In the third area, that of secrecy, I can offer no

⁶⁶⁵ *ibid* at para 21

⁶⁶⁶ *R. v. Lodhi* 2006 NSWSC 587.

⁶⁶⁷ *ibid* at para 70.

magic solution. There is likely to be an increasing presence of ASIO agents in relation to the collection of evidence to be used in criminal trials involving terrorism. Yet our intelligence agency, for all its skill in intelligence gathering, is perhaps not well equipped to gather evidence for a criminal trial; and its individual agents are not well tutored in the intricacies of the criminal law relating to procedure and evidence. Moreover, the increasing presence of our intelligence agency in the investigating and trial processes brings with it an ever increasing appearance of secrecy which, if not suitably contained, may substantially entrench upon the principles of open justice and significantly dislocate the appearance and the reality of a fair trial.⁶⁶⁸

In other words, he confirmed that establishing a workable relation between intelligence and evidence is a critical priority for future terrorism trials. He expressed concerns that the need to maintain the secrecy of intelligence would place strains on the criminal trial process. This latter challenge is particularly acute because of the increasing presence of intelligence agencies in terrorism prosecutions.

5. Summary

The Australian experience, like that of the United States and the United Kingdom, provides valuable information for reforming s.38 of the CEA so as to better manage the relation between secret intelligence and evidence or information that should be disclosed to ensure a fair trial. All three foreign jurisdictions allow the trial judge to decide questions of non-disclosure. This allows issues of non-disclosure to be integrated with comprehensive pre-trial management of a range of disclosure and other issues. Even more importantly, it allows a trial judge who has seen the secret material to revisit an initial non-disclosure order in light of the evolving issues at the criminal trial, a fact that has been emphasized by both the House of Lords and the European Court of Human Rights as essential for the fair treatment of the accused.

The comparative experience also reveals some interesting procedural innovations. British courts have held open the possible use of special

⁶⁶⁸ Justice Whealy "Terrorism" prepared for a conference for Federal and Supreme Court Judges, Perth 2007.

advocates in public interest immunity proceedings, while also indicating some awareness that delay may be caused as the special advocate becomes familiar with the case and that ethical problems may emerge from restrictions on the special advocate in communicating with the accused after the special advocate has seen the secret information. Both the United States and Australia provide for the alternative of defence counsel themselves being able to examine the sensitive material contingent on obtaining a security clearance. Although the process of obtaining a security clearance could cause delay and adversely affect choice of counsel, it also allows the person most familiar with the accused's case to have access to secret material in order to make arguments about whether its disclosure is necessary for a fair trial. Security clearance requirements may also encourage the use of experienced defence lawyers in terrorism trials. The Australian experience also suggests that the creative use of testimony by closed-circuit television can help in reconciling competing interests in disclosure and fairness when members of foreign or domestic intelligence agencies testify in terrorism prosecutions.

Conclusions

A) The Evolving Relation Between Intelligence and Evidence

What might be seen as intelligence at one point in time, might be evidence at another point in time.⁶⁶⁹ There is a need to re-examine traditional distinctions between intelligence and evidence in light of the particular threat and nature of terrorism and the expanded range of crime associated with terrorism. Terrorism constitutes both a threat to national security and a crime. Although espionage and treason are also crimes, the murder of civilians in acts of terrorism such as the bombing of Air India Flight 182 demands denunciation and punishment that can only be provided by the criminal law. The same is true with respect to intentional acts of planning and preparation to commit terrorist violence. Although attempts and conspiracies to commit terrorist violence have always been serious crimes, the 2001 *Anti-Terrorism Act* has changed the balance between intelligence and law enforcement matters by creating a wide range of terrorist offences that can be committed by acts of preparation and support for terrorism which will occur long before actual acts of terrorism. The prevention of terrorism must remain the first priority, but

⁶⁶⁹ Fred Manget "Intelligence and the Criminal Law System" (2006) 17 *Stanford Law and Public Policy Review* 415 at 421-422.

wherever possible, those who plan, prepare or commit acts of terrorism should be prosecuted and punished. Both Canada's domestic laws and its international obligations demand the prosecution and punishment of terrorism.

There is some concern that CSIS continues to resist the need to gather information in counter-terrorism investigations to evidentiary standards. In contrast, MI5 has the disclosure of information relating to the prevention of serious crime and for criminal proceedings as part of its statutory mandate and it has stated that it will gather some evidence relating to surveillance to evidential standards. With respect to Air India, CSIS information in the form of wiretaps and witness interviews could have been some of the most important evidence in the case, but, unfortunately, they were destroyed in part because of CSIS's understanding of its role as a security intelligence agency that does not collect or retain evidence. The failure to retain and disclose such material can harm both the state's interests and those of the accused.

Although CSIS is not mandated to be a law enforcement agency, s.19(2) (a) of the *CSIS Act* contemplates that it will collect information that will have significance for police and prosecutors for investigations and prosecutions and that it may disclose such information to police and prosecutors. There has never been a statutory wall between intelligence and evidence or between CSIS and the police in Canada. Section 18(2) of the *CSIS Act* also contemplates that the identity of confidential sources and covert agents may also be disclosed as required in criminal investigations and prosecutions. Section 12 of the *CSIS Act* should not be taken as authorization for the destruction of information that was collected in accordance with its requirement that information only be collected to the extent that it is strictly necessary. Stark contrasts between the reactive role of the police in collecting evidence and the proactive role of CSIS in collecting intelligence drawn by the Pitfield committee and others have not been helpful. The *CSIS Act* never contemplated an impenetrable wall between intelligence and law enforcement. Although this should have been clear in 1984, it should have been beyond doubt after the Air India bombing, let alone 9/11.

B) The Case Studies: Canada's Difficult Experience with Terrorism Prosecutions

The case studies examined in this study raise doubts about whether Canadian practices and laws are up to the demands of terrorism prosecutions, particularly as they relate to the relation between intelligence and evidence and the protection of informants. The Parmar prosecution in Hamilton, the Khela prosecution in Montreal and the Atwal prosecution in British Columbia all collapsed because of difficulties stemming from the requirements that the state make full disclosure of relevant information including the identity of confidential informants. The disclosure of the affidavit used to obtain the CSIS wiretap in Atwal disclosed inaccuracies and led to the resignation of the first director of CSIS. The disclosure of the affidavit in the Parmar prosecution also revealed inaccuracies that would have allowed the defence lawyers to cross-examine those who signed the affidavit. Both the Parmar and Atwal cases involved the then novel procedure of giving the accused access to affidavits used to obtain wiretaps and it is hoped that wiretap practice has improved and adjusted to the demands of disclosure. There is an ability to edit affidavits to protect public interests in non-disclosure, but the information that is edited-out cannot be used to support the validity of the warrant. Similarly, witness protection programs have become more formalized and may have improved since the Parmar and Khela prosecutions collapsed in part because of a reluctance of informers to have their identities disclosed to the accused because of fears for their safety. Nevertheless, these cases underline the likelihood of disclosure when judged necessary for the accused to make full answer and defence and the importance of protecting informers when intelligence is used as evidence in terrorism prosecutions.

The Kevork and Khawaja terrorism prosecutions, as well as the Ribic hostage-taking prosecution, all demonstrate a different type of problem. They were all delayed and disrupted by separate national security confidentiality proceedings in the Federal Court. Section 38 places strains on the prosecution process because it requires the Federal Court to make decisions about non-disclosure without having heard the evidence in the criminal case. In turn, it places strains on a criminal trial judge who is in the difficult, if not impossible, position of deciding whether non or partial disclosure with respect to information that the accused and even the trial judge have not seen will nevertheless adversely affect the accused's right to a fair trial and full answer and defence.

The awkward s.38 procedure was only avoided in the Malik and Bagri prosecution because the experienced counsel on both sides were able to agree on an innovative approach that included inspection of CSIS material by the defence on initial undertakings that it not be shared with their clients. Without this procedure, one that may not be easily duplicated and could require defence lawyers to obtain security clearances, the Malik and Bagri prosecution could easily have been further delayed and perhaps even halted because of the litigation of s.38 issues. A stay of proceedings or another remedy might also have been entered as a response to CSIS's destruction of tapes and witness statements had the trial judge not decided to acquit the accused. In some respects, it was a minor miracle that the case reached verdict.

Attempts have been made to encourage pre-trial resolution of s.38 issues, but the *Ribic* case and the reality of late disclosure in complex cases including the *Khawaja* prosecution suggest that a terrorism prosecution could be beset by multiple s.38 applications and by multiple trips to the Federal Court and appeals to resolve these issues. The United Kingdom and the United States have much more experience with terrorism prosecutions than does Canada and it is noteworthy that they allow the trial judge to make non-disclosure decisions on the grounds of national security confidentiality. This allows such issues to be integrated into overall trial-management issues and it allows the trial judge to revisit an initial non-disclosure issue should the evolving issues at trial suggest that fairness to the accused requires disclosure. At this point, the prosecution may face the difficult choice of whether to disclose the secret information or to halt the prosecution through a dismissal of charges or a stay of proceedings. This difficult decision, however, will not be made prematurely. It will only have to be made after a fully informed trial judge has decided that disclosure is necessary to ensure fairness towards the accused.

C) Front and Back-End Strategies for Achieving a Workable Relation Between Intelligence and Evidence

Intelligence can be protected from disclosure by not bringing prosecutions or by halting prosecutions, including through a non-disclosure order issued by the Attorney General of Canada under s.38.13 of the CEA. Nevertheless, such non-prosecution strategies are not attractive in the face of deadly terrorist plots that require prosecution and punishment. Leaving aside non-prosecution, there are two broad strategies available

to deal with the challenges presented by the need to establish a workable relation between intelligence and evidence.

One broad strategy is front-end and involves changing the nature of secret intelligence to make it usable in criminal prosecutions. These changes would be directed at the practices of CSIS to ensure that where possible they collect intelligence to evidential standards in counter-terrorism investigations and that they consider source and witness protection should it become necessary to disclose the identity of confidential informants. It will also require co-operation between CSIS and the RCMP and other police forces involved in terrorism prosecutions so that Criminal Code procedures, especially with respect to wiretaps, are used when appropriate. The challenges of these front-end reforms, especially to CSIS and to foreign agencies that share information with Canada subject to caveats that the information not be disclosed, should not be underestimated.

The second strategy focuses on the back-end procedures that can be used in court to reconcile the need to keep secrets with the need to disclose material. They involve the rules governing disclosure and production obligations and evidentiary privileges. These reforms are designed to shield intelligence and other material from disclosure in all cases. Such strategies may attract Charter challenges by limiting disclosure obligations across the board and they risk being held to be over-broad in a particular case. Fortunately, back-end strategies include better-tailored procedures to adjudicate claims of national security confidentiality on the facts of specific cases. It will be suggested that this process can be made more efficient and more fair by focusing on the concrete and specific harms of disclosure of secret information and by allowing trial judges to make, and when necessary to revise, non or modified disclosure decisions.

D) Front-End Strategies to Make Intelligence Useable in Terrorism Prosecutions

1. Collection and Retention of Intelligence With Regard to Evidential and Disclosure Standards

One important front-end strategy is for security intelligence agencies to have more regard for evidentiary and disclosure standards when they collect intelligence in counter-terrorism investigations. The likelihood of prosecution and the possible disclosure or use of some forms of

intelligence as evidence has increased since CSIS was created in 1984. This is because the threat of terrorism has increased, disclosure and production standards have increased and many new crimes with respect to the support and financing of terrorism and preparation for terrorism have been created. It will be a rare counter-terrorism investigation where there is not some possibility of a crime being committed and a prosecution being appropriate. This may not necessarily be the case with counter-intelligence or counter-espionage investigations.

In some cases, intelligence agencies such as MI5 and ASIO consciously collect evidence to evidentiary standards in the expectation that their agents may be required to produce such material to the prosecution and to testify in court. The Malik and Bagri prosecutions, however, reveal that CSIS agents at that time did not collect or retain the fruits of their terrorism investigations to evidentiary standards or with a view to a prosecution. Although the acquittal avoided the need to fashion a remedy, the trial judge found that CSIS's failure to retain relevant material including not only the wiretaps but also notes of an interview with a key witness violated Malik and Bagri's rights under s.7 of the Charter. In terrorism investigations, CSIS and other intelligence agencies should constantly evaluate the likelihood of a subsequent prosecution and the effect that a prosecution could have on secret intelligence. Where possible, they should collect and retain information to evidentiary standards.

Section 12 of the CSIS Act should not have prevented the retention of properly obtained information, but some clarification of s.12 is desirable to make clear that CSIS should retain properly obtained information when it may become relevant to criminal investigations and prosecutions. One option would be to abandon the requirement in s.12 that information and intelligence be collected with respect to activities that on reasonable grounds are suspected of constituting threats to the security of Canada only "to the extent that it is strictly necessary". Such an approach, however, would sacrifice values of restraint and privacy that are protected by the "strictly necessary" standard. A better approach is to make clear that if information is properly collected under the "strictly necessary" standard, it should be retained when it might be relevant to the investigation and prosecution of a criminal offence that also constitutes a threat to the security of Canada. Another option would be to require the retention of information that may be relevant to the investigation or prosecution of a terrorism offence as defined in s.2 of the Criminal Code.

Privacy concerns raised by any increased retention of information can be satisfied by adequate review of the legality of its collection, including the requirement that the collection be “strictly necessary” to investigate activities that may on reasonable grounds be suspected of being threats to the security of Canada. The Inspector General of CSIS, the Security Intelligence Review Committee and the Privacy Commissioner can all review not only the collection of the information but the manner in which it is retained and the manner in which is distributed to other agencies.

Information obtained under a warrant issued under s.21 of the CSIS Act could also be retained at least for the duration of the warrant albeit with restrictions on who has access to the information and with review of any information sharing. There may be a case for judicial authorization and control of information collected under a s.21 wiretap warrant. Retained intelligence should be distributed when required for a criminal investigation or prosecution as contemplated under s.19(2)(a) of the CSIS Act. There may be a case for amending s.19(2) (a) to require CSIS to disclose information that may be used in a criminal investigation or prosecution to the police and to the relevant Attorney General. The idea that CSIS could exercise their present residual discretion to refuse to disclose such information in order to protect the information from disclosure is problematic. There is a danger that acts of terrorism that could have been prevented by arrests or other law enforcement activity will not be prevented if the information is not passed on to the police. Even a refusal to pass on the information does not guarantee that an accused will not seek disclosure or production if the information becomes truly relevant to a subsequent criminal prosecution. If CSIS does pass on the information, the Attorney General of Canada would still retain the option of seeking a non-disclosure order for the secret information or issuing a non-disclosure certificate under s.38 of the CEA in order to prevent the harms of disclosure.

Although the Air India investigation had unique features that led to CSIS being held to be subject to disclosure and retention of evidence obligations under *Stinchcombe*, it would be a mistake for CSIS to conclude that the fruits of its counter-terrorism investigations could be absolutely protected from disclosure or that CSIS has a discretionary veto on disclosure requirements. Even if CSIS is considered to be a third party for purposes of disclosure, the accused in a terrorism trial may be able to make demands for disclosure of some CSIS material. The courts will impose a slightly higher standard on the accused to obtain production

from CSIS as a third party under *O' Connor* than as part of the Crown under *Stinchcombe*, but the courts will still require production when it is required to ensure fairness to the accused.

Some changes in the organizational culture of Canada's security intelligence agencies may be required to deal with the challenges of terrorism prosecutions. The need to protect secrets takes on a new dimension when the targets of intelligence are about to blow airplanes out of the sky. Intelligence agencies must adapt to the new threat environment and the increased possibility that their counter-terrorism investigations may reach a point where it is imperative that the police arrest and prosecute people. Security intelligence agencies must resist the temptation to engage in over-classification and unnecessary claims of secrecy. It is not good enough for security intelligence agencies which are increasingly focusing on counter-terrorism to rely on old mantras that they do not collect evidence.

Security intelligence agencies need to adjust their approaches to disclosure and secrecy to take into account that terrorism is now considered to be the greatest threat to national security and that they will often work along side the police in trying to prevent terrorist violence. Mechanical and broad approaches to secrecy may have been appropriate during the Cold War when the greatest threat to national security came from Soviet spies, but they are not appropriate in counter-terrorism investigations where the prospect of arrest and prosecution looms large. Starting with the Air India investigation and the *Atwal* case, CSIS has not had a happy experience with disclosure of information to the courts and it must put this unhappy experience behind it. Because of Canada's status as a net importer of intelligence, there may be tendency to err on the side of secrecy over disclosure. Nevertheless, the courts have since *Atwal* placed demands on CSIS for disclosure. More recently, courts are re-examining Cold War concepts such as the fear that a hostile state will piece together various bits of innocuous information through the mosaic effect. They are also recognizing that Canada can ask its allies under the third party rule to consent to the disclosure of intelligence and that the third party rule does not apply to information that is already in the public domain.⁶⁷⁰ All of these changes point in the direction of the increased disclosure of intelligence in the future.

⁶⁷⁰ *Canada v. Commission of Inquiry* 2007 FC 766; *Canada v. Khawaja* 2007 FC 490.

Evidentiary standards and disclosure to the court and to the accused, however, will not be possible in all cases. Security intelligence agencies must respect their statutory mandate which is to provide secret intelligence to warn the government about security threats and not to collect evidence. In addition, they must also respect restrictions on the use of intelligence that is provided by foreign agencies and they must protect their confidential informers and their agents. The protection of such information will require back-end strategies to ensure non-disclosure. More effort needs to be made by security intelligence agencies to understand the ability of the legal system to protect secrets from disclosure and to educate other actors and the public about the legitimate needs for secrecy. Justice O'Connor has warned that overclaiming of national security confidentiality could create public suspicion and cynicism about secrecy claims.⁶⁷¹ There needs to be better understanding about the legitimate need to keep secrets with respect to intelligence from our allies, ongoing investigations, secret methods and vulnerable informants.

2. Seeking Amendments of Caveats under the Third Party Rule

Canada's status as a net importer of intelligence will continue to present challenges for the management of the relation between intelligence and evidence. Canada must encourage foreign governments to share intelligence with Canada and it must respect caveats or restrictions that foreign states place on intelligence that they share with Canada. That said, the third party rule that honours caveats is not an absolute and static barrier to disclosure when required for terrorism prosecutions. The third party rule simply prohibits the use and disclosure of intelligence without the consent of the agency that originally provided the information.

A front-end strategy that can respond to the harmful effects of caveats on terrorism prosecutions is to work with foreign partners to obtain amendments to caveats that restrict the disclosure of information for purposes of prosecution. Much intelligence that the police receive from foreign and domestic intelligence agencies contains caveats that restrict the subsequent use of that intelligence in prosecutions. The Arar Commission has recently affirmed the importance of such caveats, as

⁶⁷¹ Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar *Report of the Events Relating to Maher Arar Analysis and Recommendations* (Ottawa: Public Works and Government Services) at pp 302, 304

well as the need to ensure that intelligence is accurate and reliable. At the same time, it also made clear that amendments to caveats can be sought and obtained in appropriate cases.⁶⁷² The recent decision in *R. v. Khawaja*⁶⁷³ has indicated that the third party rule should not be applied in a mechanical fashion to prevent disclosure of information that was already possessed by Canada or was in the public domain. Even when the third party rule applies, Canada should request permission from foreign agencies to allow the disclosure of information for the limited purposes of terrorism prosecutions. The idea that relationships with foreign agencies or that Canada's commitment to the third party rule will be shaken by even requesting amendments to caveats should be rejected. Foreign agencies who are also facing demands for disclosure in terrorism prosecutions in their own countries, should understand that a request to amend the caveats that they placed on information demonstrates respect for the caveat process. In some cases, foreign agencies may consent to the disclosure or partial disclosure of intelligence. The time lag between the initial collection of intelligence and its possible disclosure in a subsequent terrorism prosecution may allow caveats to be lifted or amended. In other cases, the foreign agencies will refuse to amend caveats that restrict the subsequent disclosure of information. In such cases, Canada has the tools necessary, including the use of a certificate under s.38.13 of the CEA, to honour its commitments to allies.

3. Greater Use of Criminal Code Wiretap Warrants

Another front-end strategy is to make greater use of Criminal Code authorizations for electronic surveillance in terrorism investigations where prosecutions are expected. The use of such warrants would avoid the questions of whether electronic surveillance conducted by CSIS, the CSE or foreign intelligence agencies would be admissible in Canadian criminal trials. The ATA has made it easier to obtain Criminal Code electronic surveillance warrants in terrorism investigations by eliminating a requirement to establish investigative necessity and extending the duration and notification requirements of the warrants. Such a strategy will, however, require close co-operation between CSIS and the police and a willingness to allow the police to take the lead in a terrorism investigation where grounds exist for obtaining a Criminal Code wiretap warrant.

⁶⁷² Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar *Report of the Events Relating to Maher Arar Analysis and Recommendations* (Ottawa: Government Services, 2006) at 318-322, 331-332.

⁶⁷³ 2007 FC 490 rev'd on other grounds 2007 FCA 342.

Criminal Code authorizations present their own challenges relating to the need to disclose much of the information used to obtain the judicial authorization, but the rules relating to disclosure and admissibility are clearer than with respect to security intelligence. The Part VI scheme has been upheld as constitutional by the Supreme Court and the rules and procedures for editing the affidavit to protect public interests in non-disclosure are clear. The same cannot be said about the scheme for CSIS wiretaps which were held to be constitutional in a divided decision by the Federal Court of Appeal twenty years ago.⁶⁷⁴ That said, the grounds for editing the affidavit used to obtain a wiretap warrant under s.187(4) of the Criminal Code could perhaps be expanded to allow the deletion of material that would reveal and prejudice intelligence gathering techniques even if disclosure would not endanger the persons engaged in those techniques. Other Criminal Code warrants may also be used in terrorism investigations and judges can order that information relating to such warrants not be disclosed for various reasons listed under s.487.3 of the Criminal Code. These grounds are open-ended and include protection for confidential informants and ongoing investigations, but could be expanded to include the need to protect intelligence gathering techniques. State interests in secrecy will have to be reconciled with competing concerns about open courts and fairness to the accused in the particular circumstances of each case. Criminal Code warrant procedures provide an established and constitutional basis for the reconciliation of the competing interests. Material that is edited out of the affidavit used to obtain the warrant and not disclosed to the accused cannot generally be used to sustain the warrant. As will be suggested below, security cleared special advocates could be given access to the unedited affidavit and other relevant material in order to represent the accused's interests in challenging both Criminal Code and CSIS warrants. Such an approach could help protect intelligence and other sensitive material from disclosure to the accused while allowing it to be subject to adversarial challenge.

In appropriate cases the state should continue, as it did in the *Atwal* case, to argue for the admissibility of security intelligence intercepts in criminal trials. These arguments will have a better chance of success in cases where the intelligence was gathered as a part of the intelligence mandate and "the Rubicon" had not been crossed into law enforcement activity. Although Criminal Code authorizations may be possible and helpful in some cases,

⁶⁷⁴ *R. v. Atwal* (1987) 36 C.C.C.(3d) 161 (Fed.C.A.).

intelligence agencies still have an important regulatory mandate to collect intelligence through their own special standards. In appropriate cases, intelligence intercepts could be admitted as evidence in criminal trials on the basis that the law authorizing the search is reasonable or that any departure from regular criminal law standards can be justified under s.1 of the Charter given the primary objective of collecting information to inform the government of threats to the security of Canada.

It may also be advisable to amend s.21 of the CSIS Act to make clear that a warrant can be issued to CSIS to conduct electronic surveillance outside Canada. It may be preferable to have CSIS conduct such operations with the consent of the foreign country than to rely on the foreign agencies to conduct such surveillance. The activities of the foreign agency will not be bound by the Charter and they may not have the same priorities or procedures as CSIS. An extra-territorial CSIS warrant can apply to the activities of Canadians who are terrorist suspects whereas CSE will be limited by its mandate to collect foreign intelligence. CSE intelligence gathered under a Ministerial authorization is less likely to be admitted as evidence than CSIS intelligence gathered under a judicial warrant.

Even if the use of an intelligence intercept or a Criminal Code wiretap was found by the courts to result in an unjustified violation of rights against unreasonable search and seizure, the evidence obtained could in some cases still be admitted into a criminal trial under s.24(2) of the Charter. The *Parmar* prosecution might have continued had the state been able to rely on section 24(2). The state could have argued that it relied in good faith on the warrant even if the warrant could not be sustained and was invalid after the information in the affidavit that identified the informant was edited out. Section 24(2) will not, however, work in all cases and might not have worked in *Parmar* if the court had concluded that there was a serious violation of the Charter.

4. Greater Use of Source and Witness Protection Programs

A final front-end strategy to make intelligence more usable in criminal prosecutions is the use of enhanced witness protection programs by both security intelligence agencies and police forces. Such programs are designed to make it possible for confidential informants when necessary to have their identity disclosed and to testify in criminal prosecutions. They should also when necessary provide protection to informants who may not testify but whose identity might be revealed by

disclosure requirements. The *Parmar* prosecution collapsed because of the unwillingness of a key informant to have his identity disclosed. Many of the disclosure problems in the *Khela* prosecution stemmed from the apparent agreement of the police that the key informant would not have to testify. Informants have many good reasons not to testify and there is no magic solution. Nevertheless, all reasonable efforts should be made to make it possible and attractive for them to testify.

Security intelligence agencies should be able to draw on the resources of witness protection programs. International relocation may be especially important in international terrorism prosecutions. Increased efforts should be made to ensure that the difficulties faced by witnesses are better understood by all. The importance of adequate and effective source and witness protection in managing the relation between evidence and intelligence cannot be easily overstated.⁶⁷⁵

E) Back-End Strategies To Reconcile The Demands of Disclosure and Secrecy

Although front-end strategies to make intelligence more usable in criminal prosecutions need to be developed, there is also a need for back-end strategies that can prevent the disclosure of information that if disclosed will result in serious harm. The disclosure of secret intelligence that is not necessary to ensure a fair trial should not occur given the compelling need to protect informants, security intelligence investigations and operations and the vital free flow of secret information from our allies. Whereas the burden of devising and implementing front-end strategies to make intelligence more useable in terrorism prosecutions fall largely on intelligence agencies and the police, the burden of back-end strategies generally fall on prosecutors, defence counsel, courts and legislatures.

1. Clarifying Disclosure and Production Obligations

One back-end strategy is to clarify the extent of disclosure requirements on the Crown and to provide legislative guidance for requests for

⁶⁷⁵ The most recent annual report on the federal witness protection run by the RCMP indicates that \$1.9 million was spent on it and while fifty-three people were in the program, fifteen witnesses refused to enter it, twenty-one voluntarily left the program and seven were involuntarily removed from the program. Witness Protection Program Annual Report 2005-2006 at <http://securitpublique.gc.ca/abt/dpr/le/wppa2005-6-en.asp> See also Yvon Dandurand "Protecting Witnesses and Collaborators of Justice in Terrorism Cases" in vol 3 of the Research Studies.

production from CSIS when it is determined to be a third party not subject to *Stinchcombe*. A number of the terrorism prosecutions examined in this study were undertaken before the Supreme Court's landmark decision in *Stinchcombe* which requires disclosure of relevant and non-privileged evidence or the Court's recognition in *O'Connor* of a procedure for producing and disclosing material from third parties when required for a criminal trial. Although disclosure standards existed under the common law before *Stinchcombe*, there is a need for as much clarity as possible about the extent of disclosure requirements. Some clarity has been achieved as a result of the amendments governing the opening of the sealed packet under Part VI of the Criminal Code, but more work remains to be done. In its late 1990's study of RCMP/CSIS co-operation, SIRC reported perceptions that any information that CSIS passed to the RCMP would be subject to *Stinchcombe* disclosure requirements. Although *Stinchcombe* imposes broad disclosure obligations, those obligations are not unlimited. The Crown need only disclose information that is relevant to the matters raised in the prosecution. The standard of relevance is higher with respect to *O'Connor* demands for production from third parties. In addition, some balancing of interests is allowed before disclosure of third party records. Information protected by privilege such as the informer privilege, is generally not subject to disclosure. Disclosure can be delayed for legitimate reasons relating to the safety of witnesses and sources and ongoing investigations. Finally, the courts have distinguished between violations of rights to disclosure and more serious violations of the right to full answer and defence.

There is a need for better understanding and codification of disclosure principles. Given the breadth of terrorism offences and the value of having universal rules that apply to all crimes, it may be advisable to codify disclosure principles for all prosecutions. *Stinchcombe* was decided more than fifteen years ago and even at that time, the Court seemed to expect some subsequent codification of the details of disclosure. Greater certainty about the ambit of disclosure requirements and the legitimate reasons for not disclosing information would assist in terrorism prosecutions. The comparative experience of the United Kingdom suggests that there may be considerable advantage in codifying disclosure obligations. The courts in that country proclaimed broad common law standards of disclosure in part out of a recognition that a failure to make full disclosure had resulted in miscarriages of justice in a number of terrorism cases. Parliament, however, subsequently clarified disclosure obligations and the Crown now need not disclose material in any case, including secret intelligence

in terrorism cases, unless it can reasonably be capable of undermining the case for the prosecution against the accused or of assisting the case for the accused.⁶⁷⁶ In short, it is not necessary in the United Kingdom to disclose unused but incriminating intelligence.

It will be more difficult to codify and restrict disclosure standards in Canada than in the United Kingdom because the courts have held that the accused has a constitutional right under s.7 of the Charter to disclosure of relevant and non-privileged information. The courts will accept the need to protect legitimate secrets as an objective that is important enough to justify restricting Charter rights, but the critical issue will be whether restrictions on disclosure are the most proportionate means of advancing this important objective. Courts may well look to the process under ss.37 and 38 of the CEA as a less drastic and more tailored means to secure non-disclosure of secrets by judicial order after a judge has examined the secret material in light of the facts of the particular case.

It is also possible for Parliament to legislate in relation to the procedure and standards to be applied when the accused seeks production and disclosure of records held by third parties. Although CSIS was held to be subject to *Stinchcombe* in the unique circumstances of the Air India investigation, it may be held to be a third party in other cases. Legislation to deem CSIS to be a third party not subject to *Stinchcombe* is also a possibility, but one that could be challenged under s.7 of the Charter on the facts of individual investigations. In cases where CSIS is a third party not subject to *Stinchcombe*, the Court in *Mills* made clear that Parliament can alter the common law procedure in *O'Connor* which requires the accused to show that material is likely relevant and that the interests in disclosure are greater than the interests in non-disclosure. For example, it might be possible to clarify that matters relating only to the internal workings of intelligence agencies are not relevant enough to require disclosure to the defence. It may also be possible to instruct courts to consider certain factors, such as the harmful effect of disclosure on informants, commitments made to foreign states and ongoing investigations before ordering production and disclosure. Nevertheless, any new scheme to govern the production of intelligence would have to comply with the accused's right to full answer and defence.

⁶⁷⁶ *R v Ward* [1993] 1 WLR 61; *Criminal Procedure and Investigations Act 1996* s.3 as amended by *Criminal Justice Act 2003*; *R. v. H and C* [2004] UKHL 3 at para 17.

The courts have already accepted that not every violation of the accused's right to disclosure will violate the even more fundamental right of full answer and defence. The courts may be prepared to accept some legislative limits on disclosure rights, especially when disclosure would harm state interests in national security. That said, the courts are also attentive to the cumulative adverse effects on the accused's right to full answer and defence when the accused is denied access to relevant information and information that could open up avenues for the defence. It is important that independent judges be the ultimate decision-maker about the disclosure of information because state officials have an incentive to maximize secrecy. As a result of noble-cause corruption or tunnel vision, state officials may fail to disclose information that may be valuable to the accused. A failure to make full disclosure has been an important factor in wrongful convictions, including in terrorism cases.

Legislative restrictions on disclosure or production will be challenged under the Charter. Even if upheld under the Charter, the accused will frequently argue that the state has failed to satisfy disclosure or production obligations codified in new legislation. Such arguments could delay terrorism prosecutions. Courts will not and should not return to earlier practices of ordering non-disclosure of intelligence material without even examining the material to determine its value to the accused.

2. Clarifying and Expanding Evidentiary Privileges that Shield Information from Disclosure

A related strategy to reduce disclosure and production obligations is the codification and expansion of privileges like the police informer privilege or the creation of a new privilege. There may be a case for some codification and perhaps expansion to make clear that CSIS informers also enjoy the benefit of police informer privilege, but there are limits to this strategy. Even the most zealously guarded privileges such as the police informer privilege are subject to innocence at stake exceptions.⁶⁷⁷ There is an understandable reluctance to create new class privileges and case-by-case privileges may provide little advance certainty about what is not to be disclosed. There is also a danger that new privileges will encourage the non-disclosure of information that is necessary for full answer and defence. If privileges are dramatically expanded, courts

⁶⁷⁷ *R. v. Leipert* [1997] 1 S.C.R. 287; *Named Person v. Vancouver Sun* 2007 SCC 43.

will likely make increased use of innocence at stake or full answer and defence exceptions to the expanded privilege. The end result may be that an expanded privilege may be less certain and perhaps even less protective of the state's interest in non-disclosure.

Placing too much reliance on legislating narrower disclosure or production rights or expanding privileges may invite both Charter challenges and litigation over whether information fits into the new categories. Rather than attempting the difficult task of imposing abstract limits in advance of the particular case on what must be disclosed to the accused and risking that such limits may be declared unconstitutional or spawn more litigation, a more practical approach may be to improve the efficiency of the process that is used to determine what must be disclosed and what can be kept secret within the context of a particular criminal trial. That said, presumptive privileges could have the benefit of providing some certainty to the agencies, in particular CSIS, that information could be shared with the police without necessarily being disclosed. Any new privilege would have to be defined with as much precision as possible and it would be subject to litigation to determine its precise ambit. It should also be subject to an innocence at stake exception.

3. Use of Special Advocates to Represent the Interests of the Accused in Challenging Warrants while Maintaining the Confidentiality of Information Used to Obtain the Warrant

Electronic surveillance can provide some of the most important evidence in terrorism prosecutions, especially in cases where it may be difficult and dangerous to use human sources. Both the *CSIS Act* and the *Criminal Code* provide means to obtain wiretap warrants. Both provisions have been sustained under the Charter, but courts have stressed that the general rule is that there should be full disclosure of the affidavits used to obtain the wiretap warrant. The affidavit can be edited to protect a broad range of public interests in non-disclosure including the protection of informants and ongoing investigations. This protection of information from disclosure, however, comes with a price. Any material that is edited out of the affidavit and not disclosed to the accused or perhaps summarized for the accused cannot be used to support the legality and constitutionality of the wiretap. Material that has been edited out and not known to the accused cannot be effectively challenged by the accused. In some cases, the editing may mean that the warrant is not sustainable and that the wiretap evidence can only be admitted if a judge determines that its

admission would not bring the administration of justice into disrepute under s.24(2) of the Charter.

The use of security-cleared special advocates in proceedings to challenge wiretap warrants may make it possible to provide adequate protection for the accused's right to challenge the warrant as part of the accused's right to full answer and defence and right against unreasonable searches while not disclosing to the accused information that would compromise ongoing investigations, confidential informants or secret intelligence. Special advocates at present play a role under immigration law security certificates, but the role that they could play with respect to challenging warrants could be less problematic. Special advocates would be standing in for the accused only for the limited purpose of challenging the search and arguing that the evidence should be excluded.⁶⁷⁸ A special advocate should be in a good position to make an effective adversarial challenge to the warrant. Indeed, the special advocate could be in a better position than the accused to challenge the warrant to the extent that the special advocate sees information that would normally be edited out. Finally, any evidence that the Crown would lead in a terrorism prosecution, including the results of a wiretap should it be found to be admissible, would still have to be disclosed to the accused to ensure a fair trial. Special advocates could act in the accused's interests in challenging the warrant, but they would not act for the accused during the actual trial.

A security-cleared special advocate could be given full access to the unedited affidavit used to obtain a warrant whereas now the accused only sees an edited version of the affidavit. The special advocate could also have access to other material that is relevant to challenging the wiretap warrant, including *Stinchcombe* material disclosed to the accused. The special advocate could in appropriate cases conduct cross-examinations on the affidavit. The special advocate's access to the full affidavit would respond to the concerns of the Supreme Court that the editing of the affidavit while necessary to protect important law enforcement interests, should be kept to a minimum.⁶⁷⁹ The special advocate could be briefed by the accused's lawyer about the case before the challenge to the warrant started. The special advocate could also under existing practice seek the

⁶⁷⁸ The Supreme Court has stressed the differences between proceedings where the basis for granting a warrant are challenged and a trial on the merits where the accused has full rights of cross-examination and the Crown must prove guilt beyond a reasonable doubt. *R. v. Pires*; *R. v. Lising* [2005] 3 S.C.R. 343 at paras 29-30.

⁶⁷⁹ *R. v. Durette* [1994] 1 S.C.R. 469

permission of the presiding judge to ask relevant questions of the accused or his counsel in order to challenge the warrant if this was necessary after the special advocate had seen the unedited affidavit. Such a process would have to be done with care particularly if the special advocate's questions could reveal the identity of an informant or an ongoing investigation. The use of a special advocate could allow the trial judge (who would also have to be authorized to see and hear the secret material) to hear full and informed adversarial challenges to the warrant without disclosing confidential information used to obtain the warrant to the accused or to the public. Information from the warrant that was admitted into evidence in the criminal trial would continue to be disclosed and challenged by the accused and not the special advocate.

4. Confidential Disclosure and Inspection of Relevant Intelligence

At present, lawyers for the accused are placed in the difficult position of making very broad claims for disclosure of intelligence that they have not seen. As will be seen in the next section, the accused's overbroad claims for disclosure are sometimes met with similarly overbroad claims of secrecy. The relation between intelligence and evidence may become more solid if both sides can be encouraged to make more informed and disciplined claims.

In the *Malik and Bagri* prosecution, defence counsel were allowed to inspect CSIS material on an undertaking that they would not disclose the information to their clients unless there was agreement with the prosecutors or a court order for disclosure. Agreement about disclosure was reached in that case and it was not necessary to litigate these issues in the Federal Court under s.38 of the CEA. In future cases, it may be advisable to allow defence counsel to be able to inspect secret material subject to an undertaking that they will not share that information with their client until disclosure has been approved by the Attorney General of Canada or the court. In such cases, there will be a need to ensure the confidentiality of the material that is disclosed and this may require the defence counsel to be provided with access to secure locations and secure equipment.

There may also be a case for requiring defence counsel to obtain a security clearance before obtaining access to secret material. Such a process could delay prosecutions and adversely impact choice of counsel. These problems should not be insurmountable if there is an experienced cadre

of defence lawyers with security clearances and with adequate facilities and funding to conduct a defence. Security clearances for defence lawyers are used in both Australia and the United States. Some of Canada's new special advocates also act as defence counsel.

In cases where a defence lawyer is not willing or able to obtain a security clearance, a security-cleared special advocate could be appointed to see the secret information and challenge the Attorney General's *ex parte* submissions for non-disclosure.⁶⁸⁰ The appointment of a special advocate would also add further delay to s.38 proceedings, albeit delay related to becoming familiar with the case and not with respect to obtaining a security clearance. The special advocate may never be as familiar with the possible uses of the undisclosed secret information to the accused as the accused's own lawyer. A special advocate could, however, effectively challenge overbroad claims of national security confidentiality and in that way produce material that could be disclosed to the accused. A special advocate would not be used, as is the case under immigration law, to challenge evidence that is not seen by the accused.⁶⁸¹ As the Supreme Court recognized in *Charkaoui*, s.38 of the CEA does not authorize the use of secret evidence not seen by the accused. Any extension of the use of secret evidence to criminal proceedings would violate the accused's right to a fair trial under ss.7 and 11(d) of the Charter. It would be difficult if not impossible to justify under s.1 given the more proportionate and more fair alternatives of obtaining selective non-disclosure orders on the basis of harms to national security or of prosecuting the accused for another terrorism or criminal offence that would not require the use of secret evidence.

Although special advocates may play a valuable role in s.38 proceedings before the Federal Court in challenging the government's case for secrecy and non-disclosure, it is not clear what, if any, role they would play when a criminal trial judge has to decide under s.38.14 whether

⁶⁸⁰ *Canada v. Khawaja* 2007 FC 463. See also *Khadr v. Canada* 2008 FC 46 and *Canada v. Khawaja* 2008 FC 560 appointing a security cleared lawyer in s.38 proceedings.

⁶⁸¹ The joint committee of the British House of Lords and House of Commons On Human Rights has been critical of the use of special advocates in other contexts, but has concluded that they are appropriate in the similar context of applications for public interest immunity. It has stated: "Public interest immunity decisions are not about whether the prosecution has to disclose the case on which it relies to the defence; rather, such decisions concern whether the prosecution is obliged to disclose material on which it does not rely, which might assist the defence. When deciding a public interest immunity claim, recourse can be had to court appointed special advocates." Joint Committee on Human Rights *Counter-Terrorism Policy and Human Rights: Prosecution and Pre-Charge Detention* July 24, 2006 at para 105.

a remedy is required to protect the accused's fair trial rights in light of the Federal Court's non-disclosure order. The security-cleared special advocate will have seen the secret information that was the subject of the non-disclosure order, but under the present law will not be able to inform the criminal trial judge about this information. The accused will not be subject to such restrictions, but will not have seen the information that was the subject of the non-disclosure order. The process would be simplified if the trial judge was allowed to see the secret information that was the subject of the non-disclosure order.

5. A Disciplined Harm-Based Approach to Secrecy Claims

There is a danger that overbroad demands for disclosure by the accused in terrorism prosecutions may be matched by overbroad demands for secrecy by the Attorney General of Canada. There have been a number of recent disputes over whether the Attorney General of Canada has engaged in overclaiming of national security confidentiality. The disputes between the Arar Commission and the Attorney General of Canada were resolved during the inquiry and by a decision of the Federal Court that authorized the release of the greater part of the disputed information.⁶⁸² Over use of national security confidentiality claims can produce public cynicism and suspicion about even legitimate claims of secrecy. When there are legitimate secrets that must be kept to protect vulnerable informants, ongoing investigations and promises to allies, there is a danger that the wolf of national security confidentiality may have been cried too often.

One means of addressing concerns about the legitimacy of national security confidentiality claims would be to narrow the ambit of s.38 which requires justice system participants to invoke its processes over a wide range of material that the government is taking measures to safeguard even if there is not a potential for actual injury to a public interest. Another means would be to specify the precise harms of disclosure to the public interest. Section 38.06 at present requires that the disclosure of the material would be injurious to national security, or national defence or

⁶⁸² *Canada v. Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar* 2007 FC 766. See also *Canada v. Khawaja* 2007 FC 490 and *Canada v. Khawja* 2008 FC 560 for expression of concern that the government has made secrecy claims where injury to national security from disclosure has not been established.

international relations. The courts have attempted to define these terms,⁶⁸³ but they remain extremely broad and vague. More precise definition of the harms of disclosure, or even specific examples of harms to national security or international relations, might help prevent overclaiming. It could also educate actors about the legitimate needs for secrecy with respect to matters such as the protection of vulnerable sources, ongoing investigations and promises made to allies that intelligence would not be disclosed or used in legal proceedings. A harm-based approach could respond to the concerns articulated by the Arar commission and some judges that the government has invoked s.38 in situations where the injury that would be caused by disclosure has not been established.

Section 38 could also be amended to recognize the evolving distinction between intelligence and evidence. The third party rule should not apply if the information was already in the public domain or known to Canadian officials. Even when the third party rule applies, the government could be required to make reasonable efforts to obtain consent from the originating agency to the disclosure of the caveated material. Courts have also recognized that claims that evidence should not be disclosed because of the “mosaic effect” should be approached with caution.⁶⁸⁴ Concerns about the mosaic effect have their origins in the Cold War and may not be as applicable in prosecutions of loosely organized non-state actors such as terrorists. Finally, the harms of non-disclosure could be specified especially in relation to the right to full answer and defence. Attention should be paid to the cumulative effects of non-disclosure on the ability of the accused to undermine the Crown’s case and advance defences, as well as on the fairness of the process.

A more restrained and harm-based approach to secrecy claims under s.38 of the CEA, perhaps accompanied by a willingness to allow defence counsel to inspect some secret material on condition of not disclosing the material to their clients without further agreement and perhaps after obtaining a security clearance, could decrease the need to litigate secrecy and disclosure issues under s.38 of the CEA. That said, the Attorney General of Canada will have to insist that some secret material not be disclosed

⁶⁸³ National security has been defined the “means at minimum the preservation in Canada of the Canadian way of life, including the safeguarding of the security of persons, institutions and freedoms” *Canada v. Commission of Inquiry* 2007 FC 766 at para 68. National defence includes “all measures taken by a nation to protect itself against its enemies” and “a nation’s military establishment”. International relations “refers to information that if disclosed would be injurious to Canada’s relations with foreign nations.” *Ibid* at paras 61-62.

⁶⁸⁴ *ibid*; *Canada v. Khawaja* 2007 FC 490

and the competing interests in disclosure and non-disclosure will have to be determined under s.38. It is important that the process for reconciling the interests in disclosure and non-disclosure be both fair and efficient.

6. An Efficient and Fair One Court Process for Determining National Security Confidentiality Claims

In my view the most important back-end strategy in managing the relationship between intelligence and evidence is to make the process for seeking non or modified disclosure orders in individual case more efficient and more fair for all parties. Such a reform will respond to the limits of front-end strategies in making it easier to use intelligence as evidence as well as responding to the limits of attempts to reduce disclosure requirements through legislation or the creation of new privileges. The s.38 process should evolve to allow trial judges to decide on the facts of the particular case whether and when disclosure of secret material is necessary for a fair trial. Such an approach follows the best practices of other democracies with more experience with terrorism prosecutions than Canada.

Although public interest immunities can be asserted before superior court trial judges under s.37 of the CEA, national security, national defence and international relations claims can only be asserted before the Federal Court under s.38 of the CEA. Criminal trial judges must respect the orders made by the Federal Court with respect to disclosure, but they also retain the right to order whatever remedy is required, including a stay of proceedings, to protect the accused's right to a fair trial. The *Kevork*, *Ribic* and *Khawaja* case studies underline the difficulties of Canada's two court structure. Although the trial judge in *Kevork* ultimately held that a fair trial was possible after the Federal Court refused to order the disclosure of CSIS material, he expressed much uneasiness about the bifurcated process. It is inherently difficult to ask a trial judge to conclude that disclosure of information that he or she has not seen is not necessary to ensure the fairness of the trial. At a minimum some way must be found to ensure that the trial judge and perhaps a security cleared lawyer can examine relevant secret information that has not been disclosed to the accused.

The *Ribic* prosecution demonstrates that s.38 issues can arise in the middle of a trial. In that case, a mistrial was declared when the issues were litigated in Federal Court and an appeal heard by the Federal Court of Appeal. A new trial was held, but the entire process took six

years to complete. Section 38 was amended in 2001 to require pre-trial notification of an intent to disclose or call classified information. Despite best efforts by all concerned, however, s.38 issues can emerge later in a criminal trial. For example, the Crown has a reviewable discretion to delay disclosure if required to protect witnesses. The accused may also wish to call evidence that might implicate s.38 of the CEA. A trial judge may have difficulty denying the accused the ability to call evidence that is necessary for full answer and defence. Although the Crown could be penalized for late disclosure, a refusal to allow the Crown to make a s.38 claim with respect to late-breaking disclosure could force it to abandon the prosecution in order to keep the information secret. The litigation of national security confidentiality claims in the Federal Court either before or during a criminal trial can threaten the viability of a terrorism prosecution. The accused has a right to a trial in a reasonable time and the public, including the jury, has an interest in having terrorism trials resolved in a timely manner. The delays in the *Khawaja* prosecution are a matter of concern especially when compared to completion of the trial of his alleged co-conspirators in Britain.

Even if delay problems can somehow be avoided through an expedited s.38 process, the two court approach places both the Federal Court and trial judges in difficult positions. The Federal court judge must attempt to determine the importance of non-disclosed information to the accused when the accused's lawyer has not seen the information and at a pre-trial stage when the issues that will emerge at trial may not be clear. The ability of the defence to make *ex parte* submissions to the Federal Court judge cannot compensate for the fact that the defence has not seen the undisclosed evidence and the trial evidence has not yet taken shape. Even the possibility that a security cleared special advocate may be appointed to challenge the government's case for non-disclosure cannot guarantee the disclosure of all information that should be disclosed. Even if the Federal Court judge had the advantage of full adversarial arguments on non-disclosure motions, the judge would still have the burden of making final decisions about non-disclosure and partial disclosure without knowing how the criminal trial might evolve. Judges who make similar non-disclosure decisions in Australia, the United Kingdom and the United States all take great comfort in the fact that they can revisit their non-disclosure decisions in light of emerging evidence and issues at trial.

The criminal trial judge is in an equally difficult position under the unique two court structure of s.38 of the CEA. The trial judge must decide that a

fair trial is possible without the disclosure of information that the accused, the accused's lawyers and likely the trial judge have not seen. Conversely, the trial judge must fashion a remedy, including perhaps a stay of proceedings, for non-disclosure of the secret information. Although the trial judge might be guided by a schedule that lists the information that was subject to the non-disclosure order, that schedule itself cannot contain identifying information that would cause injury to national security or national defence or international relations.⁶⁸⁵ Although the trial judge can issue a report to the Federal Court judge under s.38.05 and the Federal Court can apparently remain seized of the s.38 matter during the trial,⁶⁸⁶ the two court structure remains cumbersome and unprecedented outside Canada.

One possible argument in favour of the present two court system is that it provides a form of checks and balance between the two courts and ensures that the trial judge is not tainted by seeing the secret information that the Federal Court has ordered not be disclosed. No concerns have, however, been raised in other countries that judges will be influenced in their decisions by the information that they have seen, but ordered not to be disclosed. In many cases, the material will simply be intelligence that the Crown has found not to be necessary to be used as evidence. Judges are routinely trusted to disregard prejudicial but inadmissible information about the accused including coerced or unconstitutionally obtained confessions. In any event, the accused will also have the right to a trial by jury.

Canada's unique two court approach runs the risk of decisions in both the Federal Court and the trial court that either prematurely decide that disclosure is not necessary or alternatively that prematurely penalize the prosecution for failing to make disclosure that is not actually required in order to treat the accused fairly. In short, the bifurcated court structure is a recipe for delay and disaster in terrorism prosecutions.

No other democracy of which I am aware uses a two court structure to resolve claims of national security confidentiality. Australia, the United Kingdom and the United States all allow the trial judge to decide whether sensitive information can be withheld from disclosure without compromising the accused's rights. This approach is attractive because

⁶⁸⁵ *Canada v. Khawaja* 2007 FCA 342 at para 12.

⁶⁸⁶ *Canada v. Khawaja* 2008 FC 560.

it allows trial judges to make non-disclosure orders knowing that they can revise such orders if fairness to the accused demands it as the trial progresses.

A One Court Approach: Superior Trial Court or Federal Court?

Reforms of the two court Canadian approach could proceed in two directions. It is perhaps possible to give the Federal Court jurisdiction over all terrorism prosecutions. This approach, however, would require that the Federal Court be given jurisdiction to sit with a jury or it would attract challenge under s.11(f) of the Charter. The expansion of Federal Court jurisdiction or an attempt to create a new court to hear terrorism cases could also attract challenge under s.96 of the Constitution Act, 1867 as infringing the inherent core criminal jurisdiction of the provincial superior courts. The expansion of Federal Court jurisdiction to include criminal terrorism trials or the creation of a new terrorism court could be supported by an argument that terrorism, like youth justice, is a novel matter that did not exist in 1867. As such, it could be transferred away from the superior trial courts.⁶⁸⁷ Nevertheless, there are stronger arguments that terrorism has been around for a long time and that terrorism prosecutions in essence involve attempts to punish murder including conspiracy and attempted murder. From 1867 to the present, only superior trial courts in the provinces have tried murder charges before juries.⁶⁸⁸ Murder, like contempt of court and perhaps treason, sedition, and piracy, are matters within the core jurisdiction of the superior trial courts in the provinces. As such, they cannot be changed by Parliament or the provinces without a constitutional amendment. Removing jurisdiction from the provincial superior courts to try the most serious crimes, terrorist acts of murder or preparation or facilitation of such acts, could be held to violate s.96 of the Constitution Act, 1867.⁶⁸⁹ The Federal Court or a new terrorism court would still be conducting terrorist trials for traditional purposes of determining guilt and punishment as opposed to distinct purposes such as developing a system of youth justice. Even if s. 96 did not prevent a transfer of core superior court jurisdiction to another federal court, the

⁶⁸⁷ *Reference re Young Offenders* [1991] 1 S.C.R. 252.

⁶⁸⁸ See *Criminal Code* s.469.

⁶⁸⁹ *MacMillan Bloedel Ltd. v. Simpson* [1995] 4 S.C.R. 725 at para 15 ("The superior courts have a core or inherent jurisdiction which is integral to their operations. The jurisdiction which forms this core cannot be removed from the superior courts by either level of government, without amending the Constitution). (emphasis added) The dissent rejected the idea of core jurisdiction in that case, but also found that jurisdiction being removed from the provincial superior court to punish young people for contempt of court was ancillary to special powers exercised by youth courts.

power to constitute courts of criminal jurisdiction to try terrorism crimes is arguably a matter of provincial jurisdiction.⁶⁹⁰

Even if constitutionally permissible, such an approach would also require the Federal Court to develop and maintain expertise in criminal law, criminal procedure and criminal evidence matters. This could be difficult if terrorism prosecutions remain infrequent. A former general counsel to the Central Intelligence Agency, Fred Manget, has rejected calls for the Foreign Intelligence Surveillance Court (which issues foreign intelligence wiretaps) to conduct criminal terrorism prosecutions. He has argued that although the special court “operates with admirable secrecy, it was not meant to conduct trials. Instead, it was designed to establish the existence of probable cause, based only upon the government’s *ex parte* appearance. Mixing the probable cause determination with an adversarial trial could raise due process or impugn the impartiality of subsequent trials.”⁶⁹¹ In other words, it is better to build national security expertise into the existing criminal trial courts than to attempt to give a court with national security expertise but no criminal trial experience the difficult task of hearing terrorism trials.

Having terrorism prosecutions heard in the Federal Court or the creation of a new court would also raise concerns about special terrorism courts, concerns that have surrounded the Diplock courts in Northern Ireland and special courts in Ireland. One of the values of terrorism prosecutions is that they allow terrorist acts of violence to be denounced as crimes and terrorists to be punished and stigmatized as criminals. At this level, at least, terrorists should not be elevated to the status of a political challenge to the state that requires special solutions such as special courts.

A preferable approach would be to give designated judges of the superior trial court who have extensive experience with complex criminal trials the ability to determine national security confidentiality claims under

⁶⁹⁰ Peter Hogg has suggested that s.96 should not prevent the transfer of core superior court jurisdiction to another federal court. Peter Hogg *Constitutional Law of Canada* 4th ed at 7.2(e). But *MacMillan Bloedel Ltd. v. Simpson* [1995] 4 S.C.R. 725 at para 15 indicates that the core jurisdiction of the superior courts “cannot be removed from the superior courts by either level of government, without amending the Constitution.” In any event, Professor Hogg also indicates that the federal government does not have jurisdiction to constitute or establish courts of criminal jurisdiction, a matter expressly excluded from the federal power over criminal law and procedure under s.91(27) and included in the provincial power over the administration of justice under s.92(14). See *ibid* at 19.3. The only federal power that would support the creation of a new court to try terrorism cases would seem to be the somewhat uncertain residual power to make laws for peace, order and good government.

⁶⁹¹ Fred Manget “Intelligence and the Criminal Law System” (2006) 17 *Stanford Law and Public Policy Review* 415 at 428.

s.38 of the CEA during a terrorism trial. This could be done by amending the definition of a judge under s.38 to include a judge of the provincial superior court when a national security confidentiality matter arises before or during a criminal trial. Because of the need for secure facilities and training with respect to national security confidentiality, not all provincial superior court judges would have to be designated as judges under s.38 of the CEA. The Chief Justice of each provincial superior court could designate a few judges who would be able to make decisions under s.38 of the CEA for the purposes of criminal trials. This could also have the effect of allowing such a trial judge to be assigned to a terrorist case at the earliest possibility in order to help case manage complex terrorism prosecutions.

Superior court trial judges can already decide public interest immunity claims under s.37 and they should be able to learn enough about national security matters to make s.38 decisions. The Attorney General of Canada would still have the opportunity to make *ex parte* arguments to these judges about the dangers of disclosing information. These judges could also be assisted by adversarial argument on s.38 issues provided by the accused and by security-cleared special advocates who had examined the secret material. Finally, the Attorney General of Canada would still have the power under s.38.13 of the CEA to block a court order of disclosure of material that relates to national security or national defence or was received from a foreign entity.

It could be argued that the Federal Court should retain responsibility in all s.38 matters because of its expertise and the need to reassure allies that secret information will be treated with appropriate care. If this argument was accepted, it would still be possible to appoint select provincial superior courts judges as deputy judges of the Federal Court with the consent of their Chief Justice, the Chief Justice of the Federal Court and the Governor in Council.⁶⁹² Such judges would have to acquire expertise with respect to matters affecting national security confidentiality.⁶⁹³ In addition, it might be easier for provincial superior court trial judges who were designated as deputy judges of the Federal Court to use the secure facilities of the Federal Court.

⁶⁹² *Federal Court Act* s.10.1.

⁶⁹³ The designated judges could perhaps also consider CSIS warrant requests in order to maintain their experience should terrorism trials involving s.38 issues prove to be rare.

Allowing provincial superior court trial judges designated by their Chief Justice to decide national security confidentiality or public interest immunity questions would be consistent with the approaches taken in Australia, the United Kingdom and the United States. Such an approach could develop specialized expertise among a small number of trial judges with respect to all aspects of the management of terrorism trials including s.38 issues.⁶⁹⁴ Measures would have to be taken to ensure that superior court trial judges designated to decide s.38 issues that arise in a criminal trial would have the appropriate facilities and training for the storage of classified information and that they would have the opportunity to develop expertise on complex matters of national security confidentiality. If necessary, terrorism trials could under s.83.25 of the Criminal Code be prosecuted by the Attorney General of Canada in Ottawa, even if the offence is alleged to have been committed outside of Ontario.

This single court approach would allow trial judges to manage all disclosure aspects of complex terrorism prosecutions without artificial separations between s.38 matters that have to be decided in the Federal Court and other disclosure matters including those under s.37 that have to be decided by the trial judge. It would also stop the duplication of proceedings that may be caused by having preliminary disputes and appeals decided under s.38 only to have the same or similar issues potentially resurface before the trial judge under s.37 or s.38.14 of the CEA. A one court approach could help establish a solid institutional foundation for managing the difficult and dynamic relationship between secret intelligence and information that must be disclosed to the accused.

7. Abolishing Pre-Trial Appeals

A final reform to make the national security confidentiality process more efficient would be to repeal s.38.09 of the CEA which allows for decisions about national security confidentiality to be appealed to the Federal Court of Appeal with the possibility of a further appeal to the Supreme Court of Canada under s.38.1. The criminal trial process has traditionally avoided appeals of issues before or during a criminal trial because of concerns about fragmenting and delaying criminal trials.

An accused would retain the ability to appeal a non or partial disclosure

⁶⁹⁴ It could be argued that existing Federal Court judges with expertise in national security matters should also be allowed to conduct criminal trials. This, however, would require cross-appointing such judges to multiple provincial superior courts.

order as part of an appeal from a conviction to the provincial Court of Appeal as contemplated under the Criminal Code. It could be argued that the provincial Courts of Appeal do not have expertise in matters of national security confidentiality. Provincial Courts of Appeal already hear public interest immunity appeals under s.37 of the CEA. They could take guidance from the s.38 jurisprudence that has been developed and would continue to be developed in the Federal Court in non-criminal matters. Finally, the Supreme Court of Canada maintains the ultimate ability to interpret s.38 for all courts. If pre-trial appeals were abolished under s.38, most appeals would involve many matters of criminal law, procedure and evidence that are within the expertise of the provincial Courts of Appeal in addition to the s.38 issue.

The Attorney General of Canada would lose the right to appeal an order authorizing disclosure, a right that it exercised with partial success in *Khawaja*.⁶⁹⁵ It could be argued that this might prematurely sacrifice prosecutions by not allowing the Attorney General an opportunity to establish that a judge had committed legal error and ordered too much information disclosed to the accused. Nevertheless, the Attorney General of Canada would retain the right to issue a certificate prohibiting disclosure under s.38.13 of the CEA or of taking over a terrorism prosecution and entering a stay of proceedings should it conclude that the public interest would be seriously harmed by disclosure. The abolition of pre-trial appeals may require closer co-ordination between the Attorney General of Canada and those who handle terrorism prosecutions either in the provinces or through the new federal Director of Public Prosecutions. In any event, there is a need to co-ordinate these processes and the Attorney General of Canada retains the ability to prosecute terrorism offences.⁶⁹⁶

If pre-trial appeals from a s.38 determination are to be retained, however, thought should be given to providing time-limits not only for the filing of appeals, but also for the hearing of arguments and the rendering of decisions.

F) Conclusion

There is an urgent need to reform the process through which national security confidentiality claims are decided. Most of Canada's past terrorism

⁶⁹⁵ 2007 FCA 342. Note however that the error in that case might have been corrected by asking the judge to reconsider his original decision. *ibid* at paras 18, 52.

⁶⁹⁶ *Security Offences Act* R.S. 1985 c.S-7, s.2; *Criminal Code* s.83.25.

prosecutions have involved material supplied by Canadian and foreign security intelligence agencies and this trend will likely increase given the nature of international terrorism. Although some front-end reforms may make intelligence agencies more willing to disclose intelligence or even to use intelligence as evidence, some secrecy claims will be necessary to protect vulnerable informants, sources and methods and to respect restrictions on the subsequent disclosure of information.

Although there may be some benefits in codifying disclosure and production requirements, and in attempting to define material that clearly does not have to be disclosed or produced, there is a danger that restrictive disclosure and production requirements will generate Charter challenges and increased litigation over the adequacy of disclosure. It may be wiser to improve the efficiency of the process through which the government can seek orders to prohibit disclosure in specific instances. The 2006 MOU between the RCMP and CSIS contemplates the use of s.38 of the CEA to protect CSIS material. Unfortunately, the use of s.38 can threaten the viability of terrorism prosecutions through delay, pre-trial appeals and through non-disclosure orders by the Federal Court that may require a trial court to stay proceedings.

The parties to the Malik and Bagri prosecution took extraordinary and creative steps to avoid litigating issues under s.38. Such litigation in the Federal Court would have delayed and fractured a criminal trial which was already one of the longest and most expensive in Canadian history. If s.38 had been used in the Malik and Bagri prosecution, it is possible that the prosecution would have collapsed or that a stay of proceedings would have been entered under s.38.14. Proceedings also could have been stayed because of CSIS's failure to retain information that was of potential disclosure and evidential value to the accused. Although Air India was a unique case that hopefully will never be repeated, accused will continue to seek disclosure or production of the work of Canada's security intelligence agencies and information collected by our intelligence agencies may in some cases constitute important evidence in terrorism prosecutions. Front-end reforms designed to make intelligence more usable in terrorism prosecutions and back-end reforms to determine in an efficient and fair manner whether intelligence must be disclosed to the accused are required to respond to the unique and difficult challenges of terrorism prosecutions.

The trial judge should be empowered to make decisions about whether secret information needs to be disclosed to the accused. Such an approach should allow the trial judge to make disclosure and national security confidentiality decisions without the inefficiencies and potential unfairness revealed by separate Federal Court proceedings in the *Kevork, Ribic* and *Khawaja* prosecutions. The judge could decide in cases where the intelligence would not assist the accused that disclosure of the secret information was not necessary while retaining the ability to re-visit that decision if necessary to protect the accused's right to make full answer and defence as the trial evolves. Combined with front-end reforms that prepare intelligence to the extent possible for disclosure and use as evidence, a one court approach would move Canada towards the approaches used in other democracies with more experience in terrorism prosecutions. It would provide a better foundation for management of the difficult and dynamic relationship between secret intelligence about terrorist threats and evidence and information that must be disclosed in terrorist trials.

Without significant reforms, there is a danger that terrorism prosecutions in Canada may collapse and become impossible under the weight of our unique two court approach to reconciling the need for secrecy and the need for disclosure and our old habits of ignoring the evidentiary implications of the gathering of intelligence. An inability to try terrorism prosecutions on their merits will fail both the accused and the victims of terrorism.

Kent Roach is a Professor of Law with cross appointments in criminology and political science. He holds the Prichard and Wilson Chair of Law and Public Policy at the University of Toronto. In 2002, he was elected a Fellow of the Royal Society of Canada by his fellow academics. He was a former clerk for the last Justice Bertha Wilson on the Supreme Court of Canada. He has been the editor in chief of the *Criminal Law Quarterly* since 1998 and has appeared frequently as counsel for various interveners in the Supreme Court and Courts of Appeal. He is the author of nine books including *Constitutional Remedies in Canada* winner of the 1997 Owen Prize for best Canadian law book and (with R.J. Sharpe) *Brian Dickson: A Judge's Journey* winner of the 2004 Dafoe Prize for book that contributes most to the understanding of Canada. Two other of his books have been shortlisted for the Donner Prize for best public policy work.

In recent years, Professor Roach has focused much of his work on anti-terrorism law and policy. He is the co-editor of *Global Anti-Terrorism Law and Policy* (Cambridge: Cambridge University Press, 2005) and *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto: University of Toronto Press, 2001). He is also the author of *September 11: Consequences for Canada* (Montreal: McGill-Queens Press, 2003) and numerous other articles on anti-terrorism law including the 2002 McGill Law Journal Lecture and the 2005 Viscount Bennett Lecture. These lectures were subsequently published in the McGill Law Journal and the Cardozo Law Review respectively. He has appeared before committees of the Canadian Parliament, Indonesia and the United States Congress on matters related to anti-terrorism law and policy. He was also part of a legal expert group for the United Nation's Office on Drug and Crime that examined penal provisions to implement the Convention for the Suppression of Nuclear Terrorism.

Professor Roach's articles on anti-terrorism laws have been published in Australia, Canada, Egypt, Hong Kong, the Netherlands, Italy, Singapore, South Africa, the United Kingdom and the United States and have also been translated into Arabic, Chinese and Russian. He has lectured on anti-terrorism law and policy at the University of Cape Town, the University of New South Wales, the National University of Singapore, Oxford and Yale. He was a member of the five person research advisory panel for the Commission of Inquiry into the actions of Canadian Officials in Relation to Maher Arar and research director for Ontario's Inquiry into Forensic Pediatric Pathology. He served as Director of Research (Legal Studies) for the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.

Commission of Inquiry
into the Investigation
of the Bombing of
Air India Flight 182

